WIRELESS

SECURITY TECHNICAL IMPLEMENTATION GUIDE

Version 5, Release 2

15 November 2007

Developed by DISA for the DoD

This page is intentionally blank.

TABLE OF CONTENTS

Page

LIST OF TABLES

TABLE OF FIGURES

This page is intentionally blank.

SUMMARY OF CHANGES

GENERAL CHANGES

The previous release was Version 5, Release 1, 20 February 2007.

SECTION 1. INTRODUCTION

Minor editorial update.

SECTION 2. WLAN, WPAN, AND WWAN TECHNOLOGIES

Paragraph 2.2.2 Minor update to Figure 2-1.

Paragraph 2.2.3.5 Added preliminary 802.11n to list of standards.

Paragraph 2.2.3.6 Minor editorial update.

Paragraph 2.2.3.8 is a new section. It provides guidance on the WLAN security boundary and acceptable WLAN product architectures.

Paragraph 2.2.4 Replaced WIR0015 with WIR0016 for clarity. WIR0015 and WIR0016 were similar.

Paragraph 2.2.4. Changed WIR0076 and added WIR0012 to comply with DoD CIO memorandum "Policy on Use of Department of Defense (DoD) Information Systems Standard Consent Banner and User Agreement," dated 2 Nov 2007 that requires specific information be included in user agreements.

Paragraph 2.2.4 Minor editorial changes to the following requirements: WIR0125, WIR0168, WIR0180, WIR0225, & WIR0140.

Paragraph 2.2.4.2 WIR0205 was deleted. This requirement was combined with WIR0072.

Paragraph 2.5 Minor editorial update.

Paragraph 2.7 Minor editorial update.

SECTION 3. WIRELESS PED TECHNOLOGIES

Paragraph 3.4 Updated to add information on new DoD approved wireless email systems.

Paragraph 3.5.1 Minor updates throughout paragraph.

Paragraph 3.5.3 Minor editorial update.

Paragraph 3.7 Minor editorial update.

Paragraph 3.7 Minor editorial update to WIR0410 for clarity of requirement.

Paragraph 3.7.4 This is a new section. Contains all requirements that were in Appendix C, BlackBerry Appendix, in the previous version (removed from this version). Each requirement was revised so it applies to any wireless email system.

Paragraph 3.7.4 WIR1010 has been split into two requirements (WIR1010 and WIR1015) for clarity. WIR1015 is new.

APPENDIX A. RELATED PUBLICATIONS

Reference information updated.

APPENDIX B. IAVM COMPLIANCE

No changes.

APPENDIX C. LIST OF ACRONYMS

Section was Appendix D in previous version. Appendix C (BlackBerry Appendix) in previous edition has been deleted. BlackBerry requirements are now found in section 3.7.4, Additional Requirements for Wireless Push Email PEDs.

1. INTRODUCTION

1.1 Background

This *Wireless Security Technical Implementation Guide* (STIG) is published as a tool to assist in the improvement of the security of Department of Defense (DoD) commercial wireless information systems. The document is meant for use in conjunction with the *Enclave, Network Infrastructure, Secure Remote Computing,* and appropriate operating system STIGs.

Use of wireless technologies can improve productivity of DoD employees; however, wireless systems and handheld devices may also introduce security vulnerabilities, which, if left unmitigated, can expose government information systems to attack. In the last five years, there has been a dramatic evolution in wireless technologies, standards, and implementation practices. These changes impact the security of both wireless and wired networks. The pace of these changes is not expected to decrease for the foreseeable future, therefore, solid security engineering practices and wireless network implementation policies are crucial to ensure that DoD wireless systems are deployed and operated in a secure manner. To that end, this STIG provides an overview of each wireless technology and the security impact associated with incorporating these wireless devices into the DoD environment.

This STIG supports the design, implementation, and management of wireless devices and networks that are used to provide email and other information technology services to mobile workers in the DoD and provides implementation guidance for DoD Directive 8100.2 and ASD-NII 2 June 2006 memorandum providing supplemental policy and guidance to DoDD 8100.2. Additional information on wireless systems can be found on the DoD Wireless Community of Practice Knowledge Management (CoP KM) Web site at http://acc.dau.mil. Select the "DoD Wireless" workspace from the main web page.

This document does not cover every wireless system or network in use, or being considered for use, in the DoD. The target is for commercial wireless systems, networks, and devices that are used to provide office type services (e.g., email, travel applications, connections to office networks) using commercially available wireless equipment and wireless carriers and operated in either office or operational/tactical environments. The intent is for the requirements in this STIG to supplement other OS and network STIGs so that a seamless security infrastructure can be maintained within the DoD enterprise.

Section 2, WLAN, WPAN, and WWAN Technologies, discusses Wireless Local Area Networks (WLAN), Wireless Personal Area Networks (WPAN), and Wireless Wide Area Networks (WWAN) (wireless broadband) network technologies and security policies. Security requirements for Personal Electronic Devices (PEDs), including cell phones, Personal Digital Assistants (PDAs), and wireless email devices are discussed in *Section 3, Wireless PED Technologies*.

1.2 Authority

DoD Directive 8500.1 requires that "all IA and IA-enabled IT products incorporated into DoD information systems shall be configured in accordance with DoD-approved security

configuration guidelines" and tasks DISA to "develop and provide security configuration guidance for IA and IA-enabled IT products in coordination with Director, NSA." This document is provided under the authority of DoD Directive 8500.1.

The use of the principles and guidelines in this STIG will provide an environment that meets or exceeds the security requirements of DoD systems operating at the Mission Assurance Category (MAC) II Sensitive level, containing sensitive information.

The Information Operations Condition (INFOCON) for the DoD recommends actions during periods when a heightened defensive posture is required to protect DoD computer networks from attack. The IAO will ensure compliance with the security requirements of the current INFOCON level and will modify security requirements to comply with this guidance.

The JTF-GNO has also established requirements (i.e., timelines), for training, verification, installation, and progress reporting. These guidelines can be found on their web site: https://www.jtfgno.mil. Initially, these directives are discussed and released as Warning Orders (WARNORDs) and feedback to the JTF-GNO is encouraged. The JTF-GNO may then upgrade these orders to directives; they are then called Communication Tasking Orders (CTOs). It is each organization's responsibility to take action by complying with the CTOs and reporting compliance via their respective Computer Network Defense Service Provider (CNDSP).

1.3 Scope

This document is a requirement for all DoD administered systems and all systems connected to DoD networks. These requirements are designed to assist Security Managers (SMs), Information Assurance Managers (IAMs), Information Assurance Officers (IAOs), and System Administrators (SAs) with configuring and maintaining security controls. This guidance supports DoD system design, development, implementation, certification, and accreditation efforts.

1.4 Writing Conventions

Throughout this document, statements are written using words such as "**will**" and "**should**." The following paragraphs are intended to clarify how these STIG statements are to be interpreted.

A reference that uses "**will**" indicates mandatory compliance. All requirements of this kind will also be documented in the italicized policy statements in bullet format, which follow the topic paragraph. This makes all "**will**" statements easier to locate and interpret from the context of the topic. The IAO will adhere to the instruction as written.

Each policy bullet includes the STIG Identifier (SDID) in parentheses that precedes the policy text and references the corresponding vulnerability check in the SRR Checklist and Vulnerability Management System (VMS). An example of this will be as follows: "(*G111: CAT II*)." Throughout the document accountability is directed to the IAO to "ensure" a task is carried out or monitored. These tasks may be carried out by the IAO or delegated to someone else as a responsibility or duty.

A reference to "**should**" indicates a recommendation that further enhances the security posture of the site. These recommended actions will be documented in the text paragraphs but not in the italicized policy bullets. All reasonable attempts to meet this criterion will be made.

1.5 Vulnerability Severity Code Definitions

Severity Category Codes (CAT) are a measure of risk used to assess a facility or system security posture. Each security policy specified in this document is assigned a Severity Code of CAT I, II, or III. Each policy is evaluated based on the probability of a realized threat occurring and the expected loss associated with an attack exploiting the resulting vulnerability.

Vulnerability Severity Codes	
Category I	Vulnerabilities that allow an attacker immediate access into a machine, allow superuser access, or bypass a firewall.
Category II	Vulnerabilities that provide information that has a high potential of giving access to an intruder.
Category III	Vulnerabilities that provide information that potentially could lead to compromise.

Table 1-1. Vulnerability Severity Code Definitions

For wireless systems and devices, policies are classified as CAT I if failure to comply may lead to an exploitation which: has a high probability of occurring; does not require specialized expertise or resources; and leads to unauthorized access to sensitive information (e.g., Classified). Exploitation of CAT I vulnerabilities allow an attacker physical or logical access to a protected asset, allows privileged access, bypasses the access control system, or allows access to high value assets (e.g., Classified).

Exploitation of CAT II vulnerabilities also leads to unauthorized access to high value information; however, additional sophistication, information, or multiple exploitations are needed. Exploitation of CAT II vulnerabilities provides information that have a high potential of allowing access to an intruder but requires one or more of the following: exploitation of additional vulnerabilities; exceptional sophistication or expertise; or does not provide direct or indirect access to high value information (e.g., Classified).

A wireless policy with a CAT III severity code requires unusual expertise, additional information, multiple exploitations, and does not directly or indirectly result in access to high value information. Exploitation of CAT III vulnerabilities provide information that potentially could lead to compromise but requires additional information or multiple exploitations, but does not provide direct access to high value information.

1.6 STIG Distribution

Parties within the DoD and Federal Government's computing environments can obtain the applicable STIG from the Information Assurance Support Environment (IASE) web site. This site contains the latest copies of any STIG, as well as checklists, scripts, and other related security information. The NIPRNet URL for the IASE site is http://iase.disa.mil/.

1.7 Document Revisions

Comments or proposed revisions to this document should be sent via e-mail to fso_spt@disa.mil. DISA FSO will coordinate all change requests with the relevant DoD organizations before inclusion in this document.

2. WLAN, WPAN, AND WWAN Technologies

2.1 Introduction

The following subsections describe the technology and security issues of wireless networking devices such as WLANs, WPANs, WWANs, RFID, FSO systems, and wireless keyboards and mice. These technologies provide authorized users with wireless access to wired network resources, including the Internet.

WLANs are generally developed as an extension to an existing wired infrastructure, although they may also be installed as standalone networks. WPANs operate in the Personal Operating Space (POS) of a user, which generally extends 10 meters in any direction. WWAN systems are typically systems that provide wireless broadband data services. These systems include Broadband Wireless Access (BWA), cellular 3G (third generation) data systems, and FSO systems.

Wireless networking technologies may also be divided into short-range (less than one mile) and long-range (one mile or greater) standards. Short-range wireless standards development has occurred in three types of systems—Institute of Electrical and Electronics Engineers (IEEE) 802.11 (WLAN) and IEEE 802.15 (Bluetooth). Directional antennas can be used to extend the range of these systems. Long-range commercial standards development has occurred primarily in cellular 3G systems and BWA (IEEE 802.16). *Section 3.2, Cellular Technologies, Protocols, and Security,* provides an overview of cellular 3G systems. However, since cellular 3G security requirements are the same as WWAN systems, refer to *Section 2.6, WWAN Technologies, Protocols, and Security for DoD policies applicable to 3G systems.*

The mobility and transmission methods used for WLANs, WPANs, and WWANs introduce security issues when used as part of or close to the DoD Enclave. To ensure security in today's wireless environments, the IAO will ensure that wireless systems are designed using a defense-in-depth (security-in-depth) approach using multiple layers of security. In accordance with DoD wireless policy and Defense Security Accreditation Working Group (DSAWG) guidance, the DAA will document approval of all wireless systems used to process DoD sensitive information prior to use. DAA approval should be based upon mission requirements and a risk assessment of the wireless device.

2.2 IEEE 802.11 WLAN Systems

The IEEE 802.11 standard defines the interoperability requirements for WLANs operating in the 2.4 and 5 GHz unlicensed bands. (Note that IEEE 802.11 systems may operate in other frequency bands in countries other then the United States.) IEEE 802.11 products provide maximum data rates from 11 Mbps to 600 Mbps. The IEEE 802.11 standards group defines the WLAN standard. There is a sub-committee or sub-group for each component of the 802.11 standard.

- IEEE 802.11a is the standard for high speed WLANs in the 5 GHz band. The standard defines data rates between 6 - 54 Mbps. The 6, 12, and 24 Mbps data rates are required for all implementations.

- IEEE 802.11b is the standard for WLANs in the 2.4 GHz band. The standard defines 1, 2, 5.5, and 11 Mbps data rates.

- IEEE 802.11e is a standard that specifies Quality of Service (QoS) for WLAN systems that require QoS support (e.g., Voice over Internet Protocol (VoIP) WLAN systems).

- IEEE 802.11g is the standard for high speed (up to 54 Mbps) WLANs in the 2.4 GHz band.

- IEEE 802.11h is a standard that specifies dynamic channel selection and transmission power control for WLAN systems. Its purpose is to minimize interference between IEEE 802.11a WLAN systems and other systems operating in the 5 GHz frequency band such as radar systems, Earth Exploration Satellite Service (EESS) systems, and Space Research Service (SRS) systems.

- IEEE 802.11i is the security specification of the 802.11 standard and consists of two components: IEEE 802.1x and Robust Security Network (RSN). See subsequent sections of this document for more information on 802.11i.

- IEEE 802.11j is the standard for WLAN systems operating in the 4.9 – 5 GHz frequency band in Japan.

- IEEE 802.11n is a draft WLAN standard that will operate in the 2.4 GHz band and will provide data rates as much as 600 Mbps. Final approval of the standard is expected in late 2006 or early 2007.

- IEEE 802.11p is a standard that defines enhancements to 802.11 required to support Intelligent Transportation Systems (ITS) applications. Also referred to as Wireless Access for the Vehicular Environment (WAVE), 802.11p will be used as the groundwork for Dedicated Short Range Communications (DSRC), a US Department of Transportation project for defining vehicle-based communication networks, particularly for applications such as toll collection, vehicle safety services, and commerce transactions via cars.

- IEEE 802.11r is an unapproved standard that defines connectivity aboard vehicles in motion.

- IEEE 802.11s is an unapproved standard for Extended Service Set (ESS) Mesh Networking. The draft standard defines an architecture and protocol that support both broadcast/multicast and unicast delivery using "radio-aware metrics over self-configuring multi-hop topologies."

- IEEE 802.1x is the Port Based Network Access Control standard. IEEE 802.1x is not part of the IEEE 802.11 standard but is the authentication implementation used in most IEEE 802.11 systems. A component of IEEE 802.1x is Extensible Authentication Protocol (EAP), which provides multiple user-based authentication methods (smart cards, Kerberos, Public Key Infrastructure (PKI), etc.). EAP is not a specific authentication mechanism but rather provides a standard framework for user authentication in WLAN systems. The most common versions of EAP include the following:

- EAP-Transport Layer Security (EAP-TLS) provides strong security, but requires use of a client certificate. Used primarily in enterprises that already have deployed a PKI infrastructure. EAP-TLS provides for certificate-based, mutual authentication of the client and the network. It relies on client-side and server-side certificates to perform authentication; dynamically generated user- and session-based keys are distributed to secure the connection. Windows XP includes an EAP-TLS client.

- EAP-Tunneling Transport Layer Security (EAP-TTLS) is an extension of EAP-TLS, which provides for certificate-based, mutual authentication of the client and network. Unlike EAP-TLS, however, EAP-TTLS requires only server-side certificates, eliminating the need to configure certificates for each WLAN client. EAP-TTLS uses TLS records to tunnel the client authentication.

- Protected Extensible Authentication Protocol (PEAP) is similar to EAP-TTLS; however, with PEAP, only EAP may be carried as a protocol inside the tunnel.

- Lightweight Extensible Authentication Protocol (LEAP) is used primarily in older Cisco WLAN access points. It encrypts data transmission using dynamically generated WEP keys, and supports mutual authentication.

- EAP-MD-5 provides only minimal authentication capability and is not recommended because of significant security vulnerabilities. EAP-MD-5 duplicates CHAP password protection.

Standard	Operating Frequency	Data Rate (Typical)	Data Rate (Max)	Range (Indoor -Typical)
802.11a	5 GHz	25 Mbps	54 Mbps	10 Meters
802.11b	2.4 GHz	6.5 Mbps	11 Mbps	30 Meters
802.11g	2.4 GHz	25 Mbps	54 Mbps	30 Meters
Draft 802.11n	2.4 GHz	200 Mbps (estimated)	600 Mbps	50 Meters (estimated)

Table 2-1. Comparison of WLAN Standards

2.2.1 IEEE 802.11 WLAN Components

To understand WLANs and their associated security, you should first understand the two basic elements of a wireless network, namely, the wireless station and the access point.

2.2.1.1 WLAN Stations/Clients

A wireless station can be a laptop, desktop PC, handheld device, or any other device that utilizes wireless communication to communicate with other network devices. Stations may be mobile, portable, or stationary and can be used to transmit data or voice via VoIP phones. Wireless

network interface cards (NICs) are manufactured in the same form factors as their wired counterpart (e.g., Personal Computer Memory Card International Association (PCMCIA) cards, Peripheral Component Interconnect (PCI) cards, Industry Standard Architecture (ISA) cards, Compact Flash (CF) cards, Universal Serial Bus (USB) cards).

2.2.1.2 Access Points

An access point is the gateway between a wireless and wired network. Access points generally consist of a radio, a wired network interface, and management software. Access point functionality can be implemented using a hardware device or an application installed in another network device (a router for example) and is configured based on architecture requirements. Some vendors have removed the management and bridging software from the access point and placed these features into a wireless switch and then all access points on the network are managed and configured from the wireless switch. In a WLAN system with wireless switches, the access points are usually called access ports and are essentially transceivers (transmitter/receiver of data) with a network interface.

The wireless network must be separated from the wired network using an authorized architecture. This separation requires placement of wireless access points and bridges into a screened subnet such as a DMZ on firewall separating intranet and wireless network. Alternatively, the site may use a Virtual LAN (VLAN) or otherwise separate the WLAN from the wired internal network with a wireless Virtual Private Network (VPN) concentrator or wireless gateway, firewall, or switch placed between the access point and the local DoD network. See Figure 2.1 in a subsequent section for one example of an approved architecture. See the Network Infrastructure STIG for further details on the configuration requirements of DMZs, firewalls, VLANs, VPNs, and other network devices.

2.2.2 Technology Overview

WLANs may utilize infrared (IR) technology, narrowband technology, or radio frequency (RF) transmission. Data is placed onto a radio wave through a process called modulation, and the carrier wave acts as the transmission medium (replacing the copper or fiber optic cable of the wired network). In addition to the 2.4 GHz Industrial, Scientific, and Medical (ISM) band, WLAN products are also available that operates in the 5 GHz Unlicensed National Information Infrastructure (UNII) band (IEEE 802.11a).

2.2.2.1 Data Transmission

WLANs transmit and receive data using several different methods. The IEEE 802.11b standard defines three different physical layers—Baseband Infrared, Frequency Hopping Spread Spectrum (FHSS), and Direct Sequence Spread Spectrum (DSSS). The IEEE 802.11a and 802.11g standards specify orthogonal frequency division multiplexing (OFDM) as the transmission method while the IEEE 802.11n standard specifies Multiple-Input Multiple-Output (MIMO) as the transmission method. IEEE 802.11g also supports DSSS in order to be interoperable with 802.11b systems.

2.2.2.1.1 Infrared

Infrared-based WLANs are best suited for wireless networks whose requirements are for use within a small group or subnetwork. Infrared signals do not penetrate solid objects, such as walls and floors in a building. There are few commercial implementations of infrared WLANs because access points and stations must be within line of sight when using this transmission method.

2.2.2.1.2 Spread Spectrum

Most WLANs use spread spectrum technology for transmission. There are two methods used for spread spectrum, FHSS and DSSS. FHSS transmissions jump between several frequencies at a pre-determined rate/interval. DSSS uses a redundant chipping code and is used by nearly all 802.11b wireless LAN radios. Radio waves using the 802.11b standard, which operates at 2.4 GHz, can easily penetrate building walls and have a coverage range of up to a few hundred feet, which is useful when the signal must traverse large areas, such as multi-floor and campus environments. FHSS and DSSS do not interoperate; the transmitter and the receiver must be configured for the same transmission method.

2.2.2.1.3 OFDM

OFDM is the modulation scheme used by 802.11a and 802.11g WLANs. This method transports data using many carrier waves, with each wave carrying part of the message. The OFDM method has the following advantages when compared to spread spectrum modulation: higher data rate over a smaller bandwidth; more non-overlapping channels; increased resistance to reflected multi-path signals; increased resistance to interference.

2.2.2.1.4 MIMO

MIMO is the transmission scheme used by the draft 802.11n standard. MIMO uses multiple receiver and transmitter antennas to transmit and receive multiple data signals. This provides increased data throughput through spatial multiplexing and increased range through spatial diversity. Each simultaneous transmitted radio signal carries a component of the data stream, which is recombined by the MIMO algorithm in the receiver.

2.2.2.2 IEEE 802.11 WLAN Topologies

2.2.2.2.1 Infrastructure WLANs

The most common WLAN operational mode is the infrastructure mode where WLAN stations connect to the wired network through access points. *Figure 2-1, Enclave WLAN Architecture*, shows an example of an infrastructure mode WLAN.

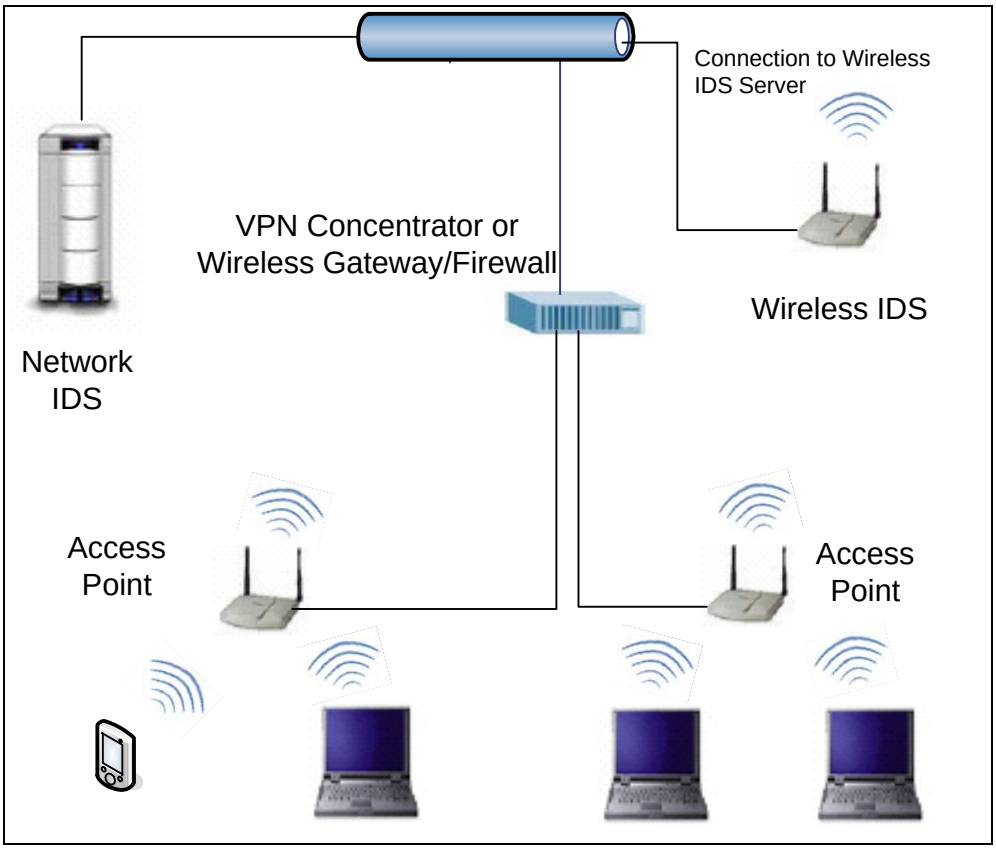

Figure 2-1. Enclave WLAN Architecture

2.2.2.2.2 Ad Hoc Wireless Networks

WLANs can be configured as a peer-to-peer (also known as ad hoc or independent) network that permits devices to communicate directly without the use of an access point. This type of implementation can be as basic as two laptops with wireless NICs transmitting data back and forth where no access point is required. Peer-to-peer WLAN communications can bypass DoD required encryption and authentication mechanisms and, therefore, these transmissions are vulnerable and could be easily intercepted, providing unauthorized access to DoD data. To mitigate this risk, peer-to-peer WLAN networks may be used only with DAA approval and will comply with requirements in Section 2.2.4 of this STIG.

2.2.2.2.3 Wireless LAN Bridges

IEEE 802.11 WLAN systems can be used to provide a wireless communications link (or bridge) between two wired LANs, typically located in adjacent buildings. The hardware used in a wireless LAN bridge is similar to a wireless LAN access point, but instead of only connecting wireless clients to the wired network, bridges are primarily used to connect other wireless LAN bridges to the network. Most wireless LAN bridges can connect to both clients and other bridge access points but the two should not be combined in operation.

2.2.3 IEEE 802.11 Wireless LAN Security

2.2.3.1 Wireless Security Overview

In general, developing a wireless network security architecture is more complicated than developing a wired network security architecture. Limits on wireless device transmission bandwidth, processing power, data storage, and mobility require that, in most cases, different security mechanisms be used to provide user authentication and data encryption. For example, the Wireless Transport Layer Security (WTLS) protocol is used to encrypt data in many wireless networks instead of Secure Socket Layer (SSL). Additionally, most Wireless Internet Service Providers (WISPs) and wireless device manufacturers preset many of the security features of the network and client devices, thus the security manager may not be able to control all security aspects of the system. When designing and implementing a wireless network and wireless security architecture, the project manager and security manager must carefully evaluate the security requirements of the system against the security features of the wireless gateway, WISP, and wireless device.

Security mechanisms for a wireless network can generally be found at three locations in the International Standards Organization (ISO) Open Systems Interconnection (OSI) 7-layer model, which is depicted in *Figure 2-2, The OSI Model.*

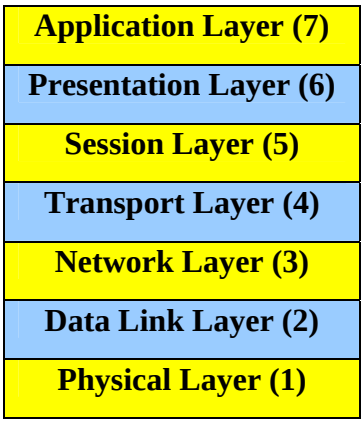

Figure 2-2. The OSI Model

At the Physical/Data Link layers many transmission protocols provide encryption and device identification. For WLANs, security services are provided by any of the following protocols: the Wired Equivalent Privacy (WEP) protocol, which is the legacy security specification of the IEEE 802.11 standard; Wi-Fi Protected Access (WPA), a legacy interim security specification; or by WPA2, the current implementation of the IEEE 802.11 security specification. For wireless PDAs, two-way email devices, and cell phones, the radio/air interface protocol may provide these services between the wireless device and the wireless service provider base station.

At the Network/Transport layers, many wireless network providers provide secure VPN tunnels using standard protocols such as IP Security (IPSec) or proprietary protocols. These secure tunnels encrypt all data between the wireless device and the wireless gateway (which may be

located at the wireless service provider or on the government operated network) and may provide device identification and/or user authentication security services.

Security is also found at the presentation and application layers where user authentication and data encryption services are offered. End-to-end security is provided between the client application on the wireless device and the application server located in the government operated network. A number of standard and proprietary protocols are used to provide these security services including SSL and WTLS. In addition, several biometric security solutions are now available including fingerprint scanning and signature recognition. For a WLAN system, security services at the application layer are usually the same as those found in the wired part of the network.

Like all IEEE 802 standards, the 802.11 standards (802.11a, 802.11b, 802.11g, and draft 802.11n) focus on the bottom two layers of the OSI model—the physical and data link layers. Security mechanisms of the 802.11 standard, such as access control and encryption, operate at the data link layer, particularly the MAC sublayer. The 802.11 MAC sublayer can work seamlessly with standard Ethernet, via a bridge or access point, to provide a connection between wireline and wireless nodes. For this reason, once the access point is reached, the same security standards supported by other 802-compliant LANs for access control (such as network operating system logins) and encryption (such as IPSec or application-level encryption) apply.

Wired Equivalent Privacy (WEP) Protocol, the original IEEE 802.11 security specification, was found to have a number of significant security vulnerabilities. Over the past three years the IEEE and the Wi-Fi Alliance industry group have released two new security specifications to improve WLAN security and interoperability. Wi-Fi Protected Access (WPA) was the first new WiFi security specification. WPA fixed a number of the known security problems with WEP but a number of security vulnerabilities remained. In early 2004 the WiFi Alliance released WPA2, which is based on the IEEE 802.11i security specification. A number of WPA2 certified products became available in late 2004. WEP and WPA do not meet DoD security requirements. WPA2 certified WLAN products are not necessarily approved for use in DoD; most are not FIPS 140-2 certified. Consult the NIST FIPS 140-2 Validated Products List prior to procuring WPA2 certified products to determine if the specific product is also FIPS 140-2 certified.

2.2.3.2 Service Set Identifier (SSID)

Although advertised as a means of simple access control for an access point or group of access points, the SSID should not be considered a safe or reliable access control mechanism. The SSID is an alphanumeric code that corresponds to a specific wireless network (or subsystem). With the default configuration of an access point, the SSID is transmitted in the clear as a part of a periodic beacon that is sent by the access point or it may be requested in a probe-request frame when a wireless client attempts to associate with an access point with a specific SSID. Most access points permit the broadcast of their identifier so that wireless stations within range know that the access point is available for a client to connect to it. Good security practice dictates that an access point should not advertise its presence and should only respond to clients that know its SSID.

2.2.3.3 MAC Address Filtering

Just as an access point or group of access points can be identified by the SSID, a client in a WLAN can be identified by the unique MAC address of its 802.11 wireless NIC. Therefore, another type of access control can be implemented based on permitting access to only those MAC addresses that are known to belong to legitimate users. Only devices having MAC addresses matching those on the list are permitted access to the WLAN. MAC related information in the header of a datagram is sent in the clear so it is possible that the MAC address can be obtained by an eavesdropper and spoofed in an attempt to gain access to the WLAN. Although MAC address filtering provides only minimal security, it should be implemented as a deterrent to the casual hacker.

MAC address filtering may not be practical for large WLAN implementations, unless the WLAN management system allows for MAC distribution lists to be centralized and automatically distributed to the point of authentication.

2.2.3.4 WEP and WPA

WEP and WPA are both "legacy" WLAN security protocols that were part of the IEEE 802.11 standard prior to the release of IEEE 802.11i. Although most consumer WLAN products and some enterprise WLAN systems continue to support these protocols, neither protocol meets DoD security requirements and will not be used in DoD.

2.2.3.5 Wi-Fi and WPA2

The Wi-Fi Alliance industry group certifies WLAN products as meeting interoperability requirements of specific WLAN standards. When a WLAN product is marked as Wi-Fi compliant, the product was evaluated by the Wi-Fi Alliance laboratory and meets the interoperability requirements found in the IEEE 802.11a, b, g or "preliminary-n" standards. The product may also be evaluated as WPA2 compliant. Note that WPA2 compliant products must be separately evaluated by NIST to determine if they are FIPS 140-2 compliant.

Products certified as WPA2 implement the requirements of the IEEE 802.11i specification, which uses a number of authentication and security protocols to establish secure wireless communications. RSN is used to establish a secure wireless connection between wireless devices. RSN uses dynamic negotiation of authentication and encryption algorithms between access points and stations. The authentication schemes are based on IEEE 802.1x and EAP with Advanced Encryption Standard (AES) as the encryption algorithm. Dynamic negotiation of the

authentication and encryption algorithms allows the use of new algorithms as they are developed. *Figure 2-3, Robust Secure Network,* details the steps of the RSN protocol.

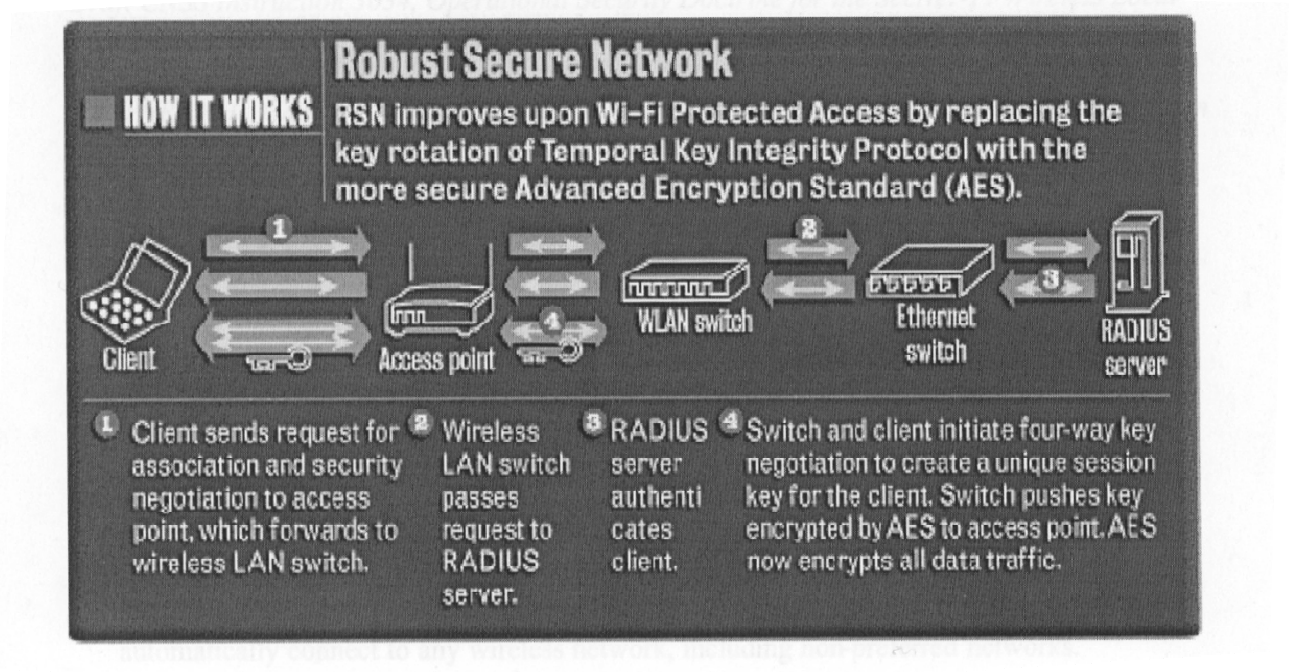

Figure 2-3. Robust Secure Network

Wireless Robust Authentication Protocol (WRAP) is an optional component of RSN that uses the Offset Codebook (OCB) mode of AES to encrypt data. Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) is the preferred encryption protocol in the IEEE 802.11i specification.

The ASD-NII Memorandum, *Use of Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies in the Department Defense (DoD) Global Information Grid (GIG),* dated 2 June 2006, specifies that, starting in FY 2007, all WLAN systems procured by DoD must meet the following requirements:

- Be WiFi Alliance certified (to ensure wireless interoperability)
- Be WPA2 certified (to ensure enterprise security interoperability)
- The encryption module of the system is validated as meeting FIPS 140-2 Level 1, at a minimum.
- If the WLAN infrastructure device (access point, bridge, wireless switch, or gateway) is used in an unprotected public area (rather than in a limited access, secure room), the encryption module of the device is validated as meeting FIPS 140-2 Level 2.

- The Advanced Encryption Standard-Counter with Cipher Block Chaining-Message Authentication Code Protocol (AES-CCMP) will be implemented in the WLAN system encryption modules.

- The EAP component of WPA2 will implement EAP-TLS mutual authentication.

- Mitigation plans for legacy WLAN systems that do not meet these requirements are reported to the DoD CIO by 29 December 2006.

2.2.3.6 Secure Wireless Networking

Harris Corporation's SecNet 11 and SecNet 54 are the only Type-1 National Security Agency (NSA) approved Secure Wireless LAN (SWLAN) systems that are approved to transmit classified data.

The SecNet 11 wireless NIC uses a Harris Sierra™ Encryption Module, Intersil PRISM™ II chipset, and Baton encryption algorithm. The card operates in the unlicensed 2.4 GHz Industrial, Scientific, and Medical (ISM) frequency band using a modified IEEE 802.11b protocol, which takes into account crypto delays. The cryptographic function is embedded in the card. SecNet 11 users can send and receive secure data, voice, and video between and among equipped wireless stations. The SecNet 11 is certified for processing classified data up to DoD Secret. The SecNet 11 only provides data encryption; it does not have any user identification or authentication capabilities. Therefore, when the SecNet 11 is used to secure a wireless LAN, additional identification and assurance equipment is needed to meet the security requirements of *DoDD 8100.2*.

The SecNet 54 can be used to secure classified data, voice, and video on both wired and wireless networks. The SecNet 54 consists of two module types: the Cryptographic Module (CMOD) and the External Module (XMOD). The CMOD provides security functionality, including Type-1 encryption. A variety of XMODs transport the encrypted data over specific data transport protocols. The initial version of the SecNet 54 includes a CMOD and a Radio Module (RMOD) that supports IEEE 802.11a, b, and g communications. SecNet 54 is certified to process classified information up to Top Secret.

NSA distributes both classified and unclassified operational keys for the SecNet 11/54 WLAN; therefore, SecNet 11/54 is available for unclassified WLANs that process sensitive information. COMSEC accounts are required for organizations that plan to use the SecNet 11/54.

The following requirements apply to SWLAN systems.

- *(WIR0200: CAT III) The IAO will ensure the CTTA is notified before installation and operation of WLANs intended for use in processing or transmitting classified data. The CTTA will designate a separation distance between secure WLAN equipment and classified processing equipment.*

- *(WIR0204: CAT I) The IAO will ensure before a SWLAN becomes operational and is connected to the SIPRNet the following occurs:*

- *The SWLAN conforms to the NSA Secure Wireless LAN CONOPS as follows:*
    - *The SWLAN architecture conforms to one of the approved Scenarios / Use Cases*
        - *SWLAN equipment is physically or electronically inventoried daily by serial number or MAC address. APs not stored in a COMSEC-approved security container are physically inventoried.*
        - *MAC filtering at the AP will be implemented. The MAC address of all approved wireless cards will be entered/stored on each AP.*
    - *SWLAN system will be rekeyed according to the following schedule:*
        - *Seaborne: Every 30 days at a minimum*
        - *Fixed Site: Every 90 days at a minimum*
        - *Airborne: Every 90 days at a minimum*
        - *Air Force Special Operations: Every 90 days at a minimum*
        - *Deployed Forces in Tactical: Every 90 days at a minimum*
- *The site SSAA is approved by the DAA and includes the SWLAN system.*
- *A SIPRNet connection approval package on file with the SIPRNet Connection Approval Office (SCAO) and/or the NIPRNet Connection Approval Process (NIPRCAP) and is updated to include the SWLAN system.*
- *Operational use/configuration of the SWLAN system is adjusted based on guidance issued by either the SCAO or NIPRCAP.*

- *(WIR0207: CAT I) The IAO will ensure wireless APs are physically secured and an alarm or alerting method is in place to detect tampering. If the SWLAN access point is not located in a limited access room, then the boundary must be controlled either with fencing or inspection. All physical cable runs must comply with guidance specified in the NAVSO P-5239-22: Protected Distribution System (PDS) Guidebook.*
- *(WIR0206: CAT III) The IAO will ensure a written operating procedure or policy exists that describe procedures for the protection, handling, accounting, and use of NSA Type-1 certified WLAN hardware and key material in a SWLAN operational environment.*
- *(WIR0180: CAT II) The IAO will ensure wireless devices are not permitted in a permanent, temporary, or mobile Sensitive Compartmented Information Facility (SCIF) unless approved in accordance with Director Central Intelligence Directive (DCID) 6/9 or 6/3 requirements.*

- *(WIR0240: CAT II) The IAO will ensure the WLAN system uses two-factor authentication for identification and authentication of the user. The WLAN device or keys/passwords stored on the WLAN device may not be used as one of the two required identification and authentication factors.*
-

Note: SecNet 11 and SecNet 54 do not currently support two-factor authentication. WIR0240 is not applicable to those products.

- *(WIR0250: CAT II) The IAO will ensure the WLAN access point is set to the lowest possible transmit power setting, which meets the required signal strength of the area serviced by the access point.*

- *(WIR0300: CAT II) The IAO will ensure wired and wireless network will be monitored by a wireless IDS or Intrusion Prevention System (IPS). The system will have the following capabilities:*

- *Continuous-scanning. The WIDS will scan continuously 24 hours/day, 7 days/week to detect authorized and unauthorized activity.*

- *Location-sensing WIDS. The WIDS will include location sensing protection scheme for authorized and unauthorized wireless devices.*

- *The WIDS are validated under the National Information Assurance Partnership (NIAP) Common Criteria as meeting U.S. Government protection profiles for basic or medium robustness environments, as determined by the DAA.*

2.2.3.7 Security Issues with Windows 2000 and XP Systems

Windows XP (and updated Windows 2000) has inherent wireless support features, provided by the Wireless Zero Configuration (WZC) service. The WZC service has a number of security vulnerabilities:

- The Automatic Network Detection and Association feature, which is enabled by default in Windows XP (pre XP SP1), causes the computer to automatically detect and attempt to associate (connect) to any wireless device that can be "seen" by the wireless NIC in the computer. The WZC service will attempt to automatically connect to wireless networks based on the networks listed in the "Preferred Networks" list. This default setting can be changed to allow the WZC service to automatically connect to any wireless network, including non-preferred networks.

- Windows 2000 and XP (pre SP2) will "leak" SSID information on any registered and approved SSID to which it has been previously connected. A list of all the access points to which the computer has ever connected is stored in XP. Upon boot-up or when out of access point range, the computer continually transmits queries, attempting to reconnect to an access point. These queries contain the SSID of all access points to which the computer has previously connected. A hacker can easily sniff the content of these queries, obtain the embedded SSIDs, and use the information to program a rogue access

point. (This is an example of why SSIDs should not be considered a good security mechanism.)

- When a third party PEAP utility is used for authentication, each 802.11-associated update to Windows XP may overwrite the PEAP settings. In most cases, the PEAP utility will have to be reinstalled.

- Windows XP SP2 provides the capability to disable WZC service from automatically connecting to wireless systems on the "Preferred Networks" list. This capability is not available with Windows 2000.

Security requirements for Windows 2000 wireless systems are as follows:

- *(WIR0163: CAT III) The IAO will ensure the WZC service is disabled in any Windows 2000 computer that is used on a WLAN. This setting should be verified whenever new software or operating system updates are installed on the computer.*

- *(WIR0164: CAT III) The IAO will ensure only WLAN drivers and WLAN management software from third party sources that do not depend on the WZC service are used in Windows 2000 computers. (Check with WLAN vendor prior to purchasing equipment.)*

NOTE: For Windows 2000 systems, the WZC service may not be used to manage WLAN connections to the computer. Instead, the WLAN software that is usually provided by the WLAN interface card vendor should be installed and used.

Security requirements for Windows XP (SP2) wireless systems are as follows:

- *(WIR0168: CAT III) The IAO will ensure if the WZC service is enabled on a Windows XP SP2 computer, the WZC service "Preferred Network" connection is configured such that the "Connect when this network is in range" selection is disabled on the Connection tab.*

2.2.3.8 Security Boundary Implementation Requirements for a DoD WLAN

The security boundary of a DoD WLAN extends from the WLAN client device to the DoD network boundary where network access is controlled. The security boundary represents the portion of the network that is most vulnerable to attack and thereby must be protected. Within this boundary there must be two distinct, but related, security protection mechanisms: authentication and data-in-transit encryption. These protections ensure access control and protection from eavesdropping for both the WLAN system and the DoD network enclave. Each security protection system must meet its security policy requirements: DODD 8100.2 for the WLAN system and DODD 8500.1 for the DoD network enclave. This section provides implementation guidance for DoD WLAN systems to ensure requirements for both DODD 8100.2 and DODD 8500.1 are met and DoD WLAN systems must meet all security requirements before a user can access the WLAN system, which in turn affords access and the DoD network enclave.

DoD network enclave security requirements dictate that strong access control be enforced prior to granting users access to the network enclave. In most cases, DoD WLAN users must use a CAC to authenticate to the DoD network enclave.
As described in requirement WIR0290, paragraph 2.2.4.1, WLAN access points, controllers, and gateways must be placed in a screened subnet or VLAN where network enclave access control mechanisms are enforced by the interface device between the wireless and wired networks. Some wireless controllers may be multi-functional, in that they not only control the authentication and encryption of the WLAN system but also act as a subnet/VLAN switch/controller and as an authentication proxy for the CAC authentication between the WLAN user and the network enclave. In this case, the wireless controller is the interface device between the wireless and wired network, and enforces the network enclave access control mechanisms.

For the WLAN system, there are a number of possible system architectures that can be used to meet the requirements set forth in the DODD 8100.2 and its supplemental memorandum policies; which states WLAN systems be WPA2 & Wi-Fi certified, FIPS 140-2 validated, and configured to support 802.1X+EAP/TLS authentication and AES-CCMP for data-in-transit encryption. Today's WLAN systems accomplish this in one of three ways including:

- Data-in-transit encryption between the WLAN client and the WLAN access point and user authentication controlled at the access point which proxies to an authentication server.
- Data-in-transit encryption between the WLAN client and the WLAN access point and user authentication controlled at a WLAN Controller/Switch/Gateway which proxies to an authentication server (or processes authentication locally).
- Encryption between the WLAN client and the WLAN Controller/Switch/Gateway (in this case, the encrypted data tunnels through the access point) and user authentication controlled at the WLAN Controller/Switch/Gateway which proxies to an authentication server (or processes authentication locally).

In each case above, the minimal security boundary protections have been met. Various implementations may be differentiated based on the location of the end points for authentication and/or data-at-rest encryption. The requirements of DODD 8100.2 and supplemental memorandum policy have been met, as long as the two security protections are in place to protect the security boundary as specified between the WLAN client device and the DoD network boundary where network access is controlled. The DoD network boundary where network access is controlled, in a DoD-owned and -operated WLAN system, is represented by the access point providing access. All points on the DoD-owned and -operated network behind the access point are access controlled. Conversely, the wireless portion of the network between the WLAN client and the access point is not access controlled. Per the DODD 8100.2 and its supplemental memorandum policy, the access point serves as the security border and controls access into the DoD network. Systems that offer an extended security boundary with the use of a WLAN Controller/Switch/Gateway are acceptable as they meet the minimum requirements.

Note: This paragraph has been included in the Wireless STIG to provide implementation guidance for ASD-NII Memorandum, Subject: Use of Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies in the Department Defense (DoD)

Global Information Grid (GIG), 2 June 2006 (referred to as the supplemental memorandum policy to DoDD 8100.2), and is not intended to replace policy found in the ASD-NII memorandum or DoDD 8100.2.

2.2.4 IEEE 802.11 WLAN Implementation Compliance Requirements

The compliance requirements in this section apply to WLAN access points, bridges (that allow wireless client connections), stations (clients), gateways and switches.

2.2.4.1 Requirements for all WLAN Systems (Classified & Unclassified)

- *(WIR0010: CAT I) The IAO will ensure all wireless systems (including associated peripheral devices, operating system, applications, network/PC connection methods, and services) are approved by the DAA prior to installation and use for processing DoD information.*

- *(WIR0016: CAT III) The IAO will maintain a list of all DAA approved wireless devices. For WLAN devices, the list will be stored in a secure location and will include the following at a minimum:*

- *Access point Media Access Control (MAC) address*
- *Access point IP address*
- *Wireless client IP address*
- *Wireless client MAC address*
- *Wireless channel set for each access point*
- *Access point DHCP range*
- *Type of encryption enabled*
- *Encryption key used*
- *Access point SSID*
- *Manufacturer, model number, and serial number of wireless equipment*
- *Equipment location*
- *Assigned users with telephone numbers*

- *(WIR0030: CAT III) The IAO will ensure wireless devices connecting directly or indirectly (e.g., hotsync, wireless) to the network are added to the site SSP.*

- *(WIR0076: CAT III) For mobile and remote users of the DoD enclave and resources, the IAM will develop a written security policy or checklist for secure wireless remote access to the site and an agreement between the site and remote user. These documents will include relevant security requirements, including (but not limited to) the following.*

- *The agreement will contain the type of access required by the user (privileged, end-user, etc.).*

- *The agreement will contain the responsibilities, liabilities, and security measures (e.g., malicious code detection training) involved in the use of the wireless remote access device.*

- *Incident handling and reporting procedures will be identified along with a designated point of contact.*

- *The remote user can be held responsible for damage caused to a Government system or data through negligence or a willful act.*

- *The policy will contain general security requirements and practices and are acknowledged and signed by the remote user.*

- *If classified devices are used for remote access from an alternative work site, the remote user will adhere to DoD policy in regard to facility clearances, protection, storage, distributing, etc.*

- *Government owned hardware and software is used for official duties only. The employee is the only individual authorized to use this equipment.*

DoD CIO Memorandum "Policy on Use of Department of Defense (DoD) Information Systems Standard Consent Banner and User Agreement," dated 2 Nov 2007 requires the following additional information in all User Agreements:

STANDARD MANDATORY NOTICE AND CONSENT PROVISION FOR ALL DOD INFORMATION SYSTEM USER AGREEMENTS
By signing this document, you acknowledge and consent that when you access Department of Defense (DoD) information systems:

- *You are accessing a U.S. Government information system (as defined in CNSSI 4009) that is provided for U.S. Government-authorized use only.*

- *You consent to the following conditions:*
  - *The government routinely monitors communications occurring on this information system, and any device attached to this information system, for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network defense, quality control, employee misconduct investigations, law enforcement investigations, and counterintelligence investigations.*
  - *At any time, the government may inspect and/or seize data stored on this information system and any device attached to this information system.*
  - *Communications occurring on or data stored on this information system, or any device attached to this information system, are not private. They are subject to routine monitoring and search.*
  - *Any communications occurring on or data stored on this information system, or any device attached to this information system, may be disclosed or used for any U.S. Government-authorized purpose.*
  - *Security protections may be utilized on this information system to protect certain interests that are important to the government. For example, passwords, access cards, encryption or biometric access controls provide security for the benefit of the government. These protections are not provided for your benefit or privacy and may be modified or eliminated at the government's discretion.*

- *(WIR0040: CAT II) The IAO will ensure all wireless devices are configured according to applicable operating system STIGs.*

- *(WIR0070: CAT III) The IAO will ensure WLAN devices installed outside of CONUS are approved by the local USFORSCOM and/or host nation.*

- *(WIR0072: CAT II) The NSO will ensure all network devices (i.e., Intrusion Detection System (IDS), routers, Remote Access System (RAS), firewalls, etc) are located in a secure room with limited access or otherwise secured to prevent tampering or theft.*

- *(WIR0075: CAT III) The IAO will ensure the organization periodically screens for unauthorized or rogue access points, stations, and bridges. Local security policy addresses the frequency for which these screenings should occur.*

NOTE: Organizations are required to perform scans regardless of whether they have an approved WLAN.

- *(WIR0140: CAT III) The IAO will ensure SSIDs are changed from the manufacturer's default to a pseudo random word that does not identify the unit, base, organization, etc. It is recommended that the SSID consist of a combination of upper and lower case characters, numbers, and special characters.*

- *(WIR0150: CAT II) The IAO will ensure the SSID broadcast mode is disabled and WLAN access points that do not allow the SSID broadcast mode to be disabled will not be used.*

- *(WIR0160: CAT III) The IAO will ensure MAC address filtering is enabled at each access point.*

- *(WIR0180: CAT II) The IAO will ensure wireless devices are not permitted in a permanent, temporary, or mobile SCIF unless approved in accordance with Director Central Intelligence Directive (DCID) 6/9 or 6/3 requirements.*

- *(WIR0225: CAT II) The IAO will ensure wireless devices are not operated in areas where classified information is electronically stored, processed, or transmitted unless:*

- *Approved by the DAA in consultation with the Certified TEMPEST Technical Authority (CTTA).*

- *The wireless equipment is separated from the classified data equipment the distance determined by the CTTA and appropriate countermeasures, as determined by the CTTA, are implemented.*

- *(WIR0230: CAT II) The IAO will ensure the wireless LAN provides a session timeout capability and the timeout is set for 15 minutes or less depending on local security policy.*

- *(WIR0250: CAT II) The IAO will ensure the WLAN access point is set to the lowest possible transmit power setting, which meets the required signal strength of the area serviced by the access point.*

- *(WIR0290: CAT II) The IAO will ensure wireless access points and bridges are placed in a screened subnet (DMZ on firewall separating intranet and wireless network) or VLAN or otherwise separated from the wired internal network by using a wireless VPN concentrator or wireless gateway/firewall/switch placed between the access point and the local DoD network.*

- *(WIR0300: CAT II) The IAO will ensure wired and wireless network will be monitored by a wireless IDS. The system will have the following capabilities:*

- *Continuous-scanning. The WIDS will scan continuously 24 hours/day, 7 days/week to detect authorized and unauthorized activity.*

- *Location-sensing WIDS. The WIDS will include a location sensing protection scheme for authorized and unauthorized wireless devices.*

- *The WIDS are validated under the NIAP Common Criteria, as meeting U.S. Government protection profiles for basic or medium robustness environments, as determined by the DAA.*

- *(WIR0330: CAT I) The IAO will ensure WLAN network device management interfaces and management consoles are password protected and the password is compliant with DoD password policies. Password length and complexity will be in accordance with requirements of current INFOCON level.*

For peer-to-peer networks the following additional requirements apply:

- *(WIR0125: CAT II) The IAO will ensure strong mutual authentication between each station on the peer-to-peer network occurs before data is transmitted between stations. IEEE 802.1x authentication with EAP-TLS is required.*

For WLAN clients the following additional requirements apply:

- *(WIR0050: CAT I) The IAO will ensure DoD licensed anti-virus software is installed on all wireless clients (e.g., laptops, PDAs, and cellular telephones) and the software is configured in accordance with the Desktop Application STIG and is kept up-to-date with the most recent virus signatures every 14 days or less. Antivirus software is NIAP Common Criteria validated as meeting U.S. Government protection profiles.*

- *(WIR0100: CAT III) The IAO will ensure a personal firewall is implemented on each 802.11-enabled wireless device to block unauthorized access to the device and the software is configured in accordance with the Desktop Application STIG. Personal firewall software is NIAP Common Criteria validated as meeting U.S. Government protection profiles.*

- *(WIR0130: CAT II) The IAO will ensure WLAN Network Interface Cards (NICs) that do not have the capability to turn off or otherwise disable peer-to-peer WLAN communications are not used.*

- *(WIR0161: CAT II) The IAO will ensure computer/PED wired network interfaces (e.g., Ethernet) are disconnected or otherwise disabled when wireless network connections are being used.*

- *(WIR0167: CAT III) The IAO will ensure laptops with WLAN cards have the WLAN card radio set to OFF as the default setting.*

- *(WIR0240: CAT II) The IAO will ensure the wireless system uses two-factor authentication for identification and authentication of the user prior to connection to any DoD network. The WLAN device or keys/ passwords stored on the wireless device may not be used as one of the two required identification and authentication factors. IEEE 802.1x authentication with EAP-TLS is required.*

2.2.4.2 Additional Requirements for Classified WLAN Systems

The DAA has the responsibility to ensure that only NSA Type-1 certified WLAN systems are used for the wireless transmission of classified information. All wireless systems will be approved and documented prior to connecting to the SIPRNet. The

- *(WIR0203: CAT I) The IAO will ensure only NSA Type-1 certified WLAN systems are used for wireless transmission of classified information.*

- *(WIR0170: CAT II) The IAO will ensure WLANs are used to store, process, or transmit classified and/or SCI information only up to the classification level the system is approved by NSA to support.*

NOTE: For example, Secret and below for SecNet 11 and Top Secret and below for SecNet 54.

- *(WIR0190: CAT II) The IAO will ensure computers with embedded WLAN systems that cannot be removed by the user are not used to store, process, or transmit classified information.*

- *(WIR0200: CAT III) The IAO will ensure the CTTA is notified before installation and operation of WLANs intended for use in processing or transmitting classified data. The CTTA will designate a separation distance between secure WLAN equipment and classified processing equipment.*

- *(WIR0204: CAT I) The IAO will ensure before a SWLAN becomes operational and is connected to the SIPRNet the following occurs:*

- *The SWLAN conforms to the NSA Secure Wireless LAN CONOPS as follows:*
    - *The SWLAN architecture conforms to one of the approved Scenarios/Use Cases.*
    - *SWLAN equipment is physically or electronically inventoried daily by serial number or MAC address. APs not stored in a COMSEC-approved security container are physically inventoried.*
    - *MAC filtering at the AP is implemented. The MAC address of all approved wireless cards is entered / stored on each AP.*
    - *SWLAN system is rekeyed according to the following schedule:*
        - *Seabourne: Every 30 days at a minimum*
        - *Fixed Site: Every 90 days at a minimum*
        - *Airbourne: Every 90 days at a minimum*
        - *Air Force Special Operations: Every 90 days at a minimum*
        - *Deployed Forces in Tactical: Every 90 days at a minimum*
- *The DAA approves the site SSAA and includes the SWLAN system.*
- *A SIPRNet connection approval package is on file with the SIPRNet Connection Approval Office (SCAO) and/or the NIPRNet Connection Approval Process (NIPRCAP) and is updated to include the SWLAN system.*
- *Operational use / configuration of the SWLAN system is adjusted based on guidance issued by either the SCAO or NIPRCAP.*

- *(WIR0206: CAT III) The IAO will ensure a written operating procedure or policy exists describing procedures for the protection, handling, accounting, and use of NSA Type-1 certified WLAN hardware and key material in a SWLAN operational environment.*

- *(WIR0220: CAT II) The IAO will ensure tools are used to encrypt classified data at rest on the wireless device. Encryption tools are NSA Type-1 certified.*

2.2.4.3 Additional Requirements for Unclassified WLAN Systems

- *(WIR0260: CAT II) The IAO will ensure all sensitive data (e.g., For Official Use Only (FOUO), Privacy Act information) stored on WLAN clients (i.e., laptops, PDAs) are encrypted using either encryption of the file system or individual files. The encryption system is FIPS 140-2 overall Level 1 or 2 validated (as directed by the DAA based on the sensitivity of the data).*

- *(WIR0270: CAT II) The IAO will ensure the WLAN system meets the following encryption and authentication requirements:*

- *The encryption modules of the WLAN equipment are validated as meeting FIPS 140-2 overall Level 1 validated (at a minimum) and the information assurance component of the WLAN system is NIAP Common Criteria validated for basic or medium robustness (as determined by the DAA). The Advanced Encryption Standard-Counter with Cipher Block Chaining-Message Authentication Code Protocol (AES-CCMP) will be implemented in the WLAN system encryption modules.*

- *If the WLAN infrastructure device (access point, bridge, wireless switch or gateway) is used in an unprotected public area, the encryption module of the device is validated as meeting FIPS 140-2 Level 2, at a minimum.*

- *The EAP component of WPA2 will implement EAP-TLS mutual authentication. (This requirement is not applicable to connections between WLAN bridges.)*

- *Mitigation plans for legacy WLAN systems that do not meet these requirements are reported to the DoD CIO by 29 December 2006.*

- *(WIR0275: CAT III) The IAO will ensure all new WLAN acquisitions; the WLAN-enabled devices (e.g., NICs and access points) that store, process, or transmit unclassified information are Wi-Fi Alliance certified and WPA2 Enterprise certified.*

- *(WIR0280: CAT II) The IAO will ensure if a WLAN device is to be used to access a DoD network via the Internet through a public WLAN/Internet gateway (e.g., airport or hotel "hotspot"), the following requirements are met:*

- *When using a PDA for remote access, the PDA compliance requirements in the Wireless STIG are followed.*

- *The requirements in the Secure Remote Computing STIG are followed.*

- *The wireless client device has an approved personal firewall, antivirus, and VPN client installed and is operational with the latest updates installed before the wireless connection is enabled.*

- *After connecting to the hotel wireless portal, users are trained to immediately connect to the DoD network via the VPN client. All connections for Government official business to the Internet via the hotel wireless network will be through the DoD VPN connection only.*

- *Users are trained to turn-off wireless cards immediately after a VPN connection is disconnected.*

Additional security requirements for Windows 2000 wireless systems are as follows:

- *(WIR0163: CAT III) The IAO will ensure the WZC service is disabled in any Windows 2000 computer that is used on a wireless LAN. This setting should be verified whenever new software or operating system updates are installed on the computer.*

- *(WIR0164: CAT III) The IAO will ensure only WLAN drivers and WLAN management software from third party sources that do not depend on the WZC service are used in Windows 2000 computers. (Check with WLAN vendor prior to purchasing equipment.)*

Additional security requirements for Windows XP (SP2) wireless systems are as follows:

- *(WIR0168: CAT III) The IAO will ensure if the WZC service is enabled on a Windows XP SP2 computer, the WZC service "Preferred Network" connection is configured such that the "Connect when this network is in range" selection is disabled on the Connection tab. In addition, the WZC setting "Automatically connect to non-preferred networks" is not selected.*

2.2.5 WLAN Common Criteria Protection Profiles

NSA has developed a suite of protection profiles (PP) focused on wireless networking technologies. For WLANs, the *U.S. Government Wireless Local Area Network (WLAN) Access System for Basic Robustness Environments Protection Profile* and *U.S. Government Wireless Local Area Network (WLAN) Client for Basic Robustness*, focus on IEEE 802.11 WLAN systems. PPs can be found at http://niap.bahialab.com/pp/index.cfm. The PPs specify minimum-security requirements for a WLAN access system and client used by the U.S. Government in basic robustness environments. The assurance specified in the Basic robustness PP is Evaluation Assurance Level (EAL) 2. The target robustness level of "basic" is specified in DoD Instruction 8500.2.

2.3 Bluetooth WPAN

2.3.1 Overview

The Bluetooth Special Interest Group (SIG), which is a group of companies interested in promoting Bluetooth wireless solutions, developed the Bluetooth specification which became the IEEE 802.15 WPAN standard. The primary goal of the specification is to define wireless connectivity for fixed, portable, and moving devices within or entering the personal operating space of the user. The goal is to achieve interoperability (e.g., no radio interference) between a WPAN device and any IEEE 802.11 WLAN device. The IEEE 802.15.1 standard defines device-level authentication at the data link layer and data encryption at the physical layer.

Bluetooth enabled electronic devices connect and communicate wirelessly via short-range (100m or less) in ad hoc networks called piconets. Bluetooth and 802.11 wireless technologies share

some characteristics and overlap slightly in some usage models, but they serve fundamentally different purposes.

Bluetooth systems can be operated in the DoD, provided they meet the security compliance requirements listed in the compliance subsections of this section. Security for a Bluetooth network can be found at both the physical and data link layers of the protocol. Bluetooth uses FHSS modulation. FHSS modulation provides a 1600 hops/sec frequency-hopping rate with low output transmission power and short transmission range (see Table 2-2).

Device Class	Strength	Range (Meters)
Class 1	100 mW	Up to 100
Class 2	2.5 mW	Up to 10
Class 3	1 mW	About 1

Table 2-2. Bluetooth Power and Range Specifications

At the data link layer, Bluetooth provides both authentication and encryption. Each Bluetooth device has a unique device address that is used to authenticate the devices. Either one-way, two-way, or no authentication may be specified. For encryption, Bluetooth uses an algorithm where the key length is selectable between 8 and 128 bits. This allows Bluetooth to be used in countries that limit the length of encryption keys. The encryption key size in a specific Bluetooth device must be set at the factory in order to prohibit the user from overriding the permitted key size.

Bluetooth has many of the same security management problems found with the IEEE 802.11b standard (pre-802.11i release) in that no process is defined for managing the process for issuing, validating, and revoking link keys. Bluetooth provides for built-in encryption and authentication, but like 802.11b, additional security products must be used to mitigate the inherent security shortcomings of the standard and meet DoD security requirements. Additional information on Bluetooth security issues can be found in NSA IA Advisory IAA 004-2004, Vulnerabilities and Countermeasures Associated with Integrated Bluetooth capability, 13 May 2004.

In addition to Bluetooth, there are several other PAN system standards defined by the IEEE 802.15 working group. The four IEEE 802.15 standards are as follows:

- IEEE 802.15.1 Bluetooth.
- IEEE 802.15.2 Coexistence. Standard that defines the coexistence between WPAN and WLAN systems.
- IEEE 802.15.3 WPAN high rate standard, WiMedia (>= 20Mbps).
- IEEE 802.15.3a WPAN ultra high rate standard, Ultra Wideband (UWB), (>= 110 Mbps).

- IEEE 802.15.4 WPAN low rate, Zigbee (20-250 Kbps). Used for sensors, interactive toys, and home automation.

2.3.2 Bluetooth Compliance Requirements

Note: Bluetooth security requirements for BlackBerry and Windows Mobile wireless email devices are found in section 3.7.4 (WIR1140 and WIR1150).

- *(WIR0010: CAT I) The IAO will ensure all wireless systems (including associated peripheral devices, operating system, applications, network/PC connection methods, and services) are approved by the DAA prior to installation and use for processing DoD information.*

- *(WIR0080: CAT II) The IAO will ensure Bluetooth devices are not used to store, process, or transmit DoD information, unless FIPS 140-2 validated cryptographic modules are used to encrypt the data during transmission.*

- *(WIR0083: CAT III) The IAO will ensure the Bluetooth capability is removed or disabled from the PED (laptop computer, PDAs, cell phones, BlackBerry devices, and etc.) if FIPS 140-2 validated cryptographic modules are not used.*

- *(WIR0180: CAT II) The IAO will ensure wireless devices are not permitted in a permanent, temporary, or mobile SCIF unless approved in accordance with DCID 6/9 or 6/3 requirements.*

- *(WIR0182: CAT I) The IAO will ensure Bluetooth devices are not used to send, receive, store, or process classified messages.*

- *(WIR0225: CAT II) The IAO will ensure wireless devices are not operated in areas where classified information is electronically stored, processed, or transmitted unless:*

- *Approved by the DAA in consultation with the CTTA.*

- *The wireless equipment is separated from the classified data equipment the distance determined by the CTTA and appropriate countermeasures, as determined by the CTTA, are implemented.*

2.4 Wireless Mice and Keyboards

Wireless keyboard and mice are increasingly used throughout the Federal Government. These devices use various wireless technologies such as WLAN, Bluetooth, and IR to transmit data to the computer. Wireless mice transmit telemetry data (right, left, etc.), while wireless keyboards transmit users' keystrokes. Note that some wireless keyboards and mice do not transmit in the WLAN, Bluetooth, or IR frequency bands. In these cases, the security requirements for WLAN systems should be followed (see WIR0132 below). The following guidance is based on testing and guidance provided by NSA.

The threat to Bluetooth and 802.11 keyboards and mice stems from two sources. First, the wireless signals from a wireless keyboard or mouse may be received by another keyboard or mouse in a nearby area. There are instances where typing on one keyboard may be picked up by a receiver attached to a nearby workstation which is also using a wireless keyboard or mouse. Second, the receiver that is attached to the USB port of the client workstation could provide a method for an attacker to breech the security of the workstation without requiring physical access to the USB port.

The DoD wireless policy requires use of FIPS 140-2 encryption to protect wireless communication; however, there are currently no wireless keyboards or mice available that meet this requirement.

- *(WIR0132: CAT II) The IAO will ensure if WLAN or Bluetooth mice and keyboards are used, applicable requirements listed in Section 2.2.4, IEEE 802.11 WLAN Implementation Compliance Requirements, or Section 2.3, Bluetooth WPAN, are followed.*

When installed and configured in accordance with the following policy, Infrared keyboards and mice can be used with workstations attached to NIPRNet or SIPRNet. Most vendors have discontinued selling Infrared keyboards or mice so these products are difficult to obtain and are only rarely used in the DoD environment.

- *(WIR0131: CAT II) The IAO will ensure if infrared wireless mice and keyboards are used on classified or unclassified equipment and networks, the following conditions are followed:*

- *The DAA, in consultation with the CTTA, has approved IR wireless mice and/or keyboards for use in the facility.*

- *When wireless mice and/or keyboards are used on classified equipment, the area is approved for processing classified information at the appropriate level.*

- *The area is totally enclosed with walls, ceiling, and floor consisting of material opaque to IR. There are no windows unless each window is covered with a film approved for blocking IR. All doors will remain closed when the devices are in operation.*

- *There is no mixing of classified and unclassified equipment using IR within the same enclosed area.*

- *When IR is used with classified equipment in the same enclosed area as unclassified equipment with IR ports, the IR ports on the unclassified equipment is completely covered with metallic tape.*

- *When IR is used with unclassified equipment in the same enclosed area as classified equipment with IR ports, the IR ports on the classified equipment is completely covered with metallic tape.*

2.5 Voice Over IP (VoIP) WLAN Systems

Wireless VoIP systems offer the convenience of a mobile or cellular phone combined with the cost savings of a VoIP telephone system.

The following conditions are to be met prior to the use of wireless VoIP systems:

- *(WIR0133: CAT II) The IAO will ensure all wireless VoIP systems comply with applicable requirements in the Wireless STIG, Section 2.2.4, IEEE 802.11 WLAN Implementation Compliance Requirements, and the VoIP STIG.*

2.6 WWAN Technologies, Protocols, and Security

2.6.1 Introduction

Commercial WWAN data services (also called wireless broadband) began to be used in the U.S. in the early 1990s as low speed (less then 30 Kbps) data networks and were used primarily for pagers, wireless PDAs, and email devices (e.g., BlackBerry). In the late 1990s wireless data broadband services (100 Kbps to 1+ Mbps) started to become available. The development and subsequent deployment of WWAN services has followed two paths: cellular based standards (3G services) and IEEE standards based services. This section discusses both legacy wireless data services and IEEE standards based WWAN services. Cellular based wireless data services are reviewed in *Section 3.2.1, Wireless Telephone Protocols*.

2.6.2 Legacy PDA Wireless Air Interface Protocols

This section describes the two most prevalent low speed radio interface protocols that have been used in the United States for PDA and laptop wireless Internet access. Wireless carriers started discontinuing these services in 2004.

- Cellular Digital Packet Data (CDPD) is an open standard for packet data service that is integrated with existing AMPS and IS-136 TDMA networks. CDPD provides data rates up to 19.2 Kbps. CDPD provides device-level authentication and data encryption between the wireless device and the carrier base station. In addition, the standard includes sophisticated anti-cloning protection. Few U.S. wireless carriers continue to operate CDPD networks and new customers are no longer accepted. Wireless carriers started discontinuing these services in 2004.

- Mobitex is an open standard for a narrow band data packet switching network that is used by several wireless PDAs and older BlackBerry email devices. Sprint Nextel is the only U.S. company that provides Mobitex service. Mobitex security primarily consists of device-level authentication using an embedded device ID number, but this number is subject to the same cloning problems as analog cellular phones. Although the standard includes data bit scrambling, this is done for technical reasons and should not be considered data encryption.

2.6.3 IEEE 802.16 BWA Technology

The IEEE 802.16 (BWA) standard defines interoperability requirements for Wireless Metropolitan Area Networks (WMANs) that operate in the 2 – 66 GHz frequency range. These networks offer subscriber local loop service (similar to a local telephone service) and wireless hotspots for Internet connections (similar to an 802.11b WLAN hot-spot) and compete with both public 802.11 and broadband 3G cellular services. BWA networks focus on the first mile/last mile connection in WMAN networks and provide broadband alternatives to DSL, cable, or T-1 services. Data rates for BWA systems vary and depend on the specific implementation but subscribers should expect data rates equal to or greater than T-1 and DSL (1.5 Mbps+).

BWA systems are usually deployed in a Point to Multipoint (PMP) topology where the base station services multiple subscribers located in the broadcast area of the base station. The base station is collocated with an entry point of the service provider's backhaul system and connects to the Internet backbone through the backhaul system. The BWA standard defines an optional topology, called Mesh Mode, for areas of high user density or areas were subscribers do not have line of sight to a base station located at the backhaul system entry point (airhead). In a mesh network, intermediate base stations (intermediate devices) have the capability to route traffic to other intermediate devices until the airhead is reached. Mesh networks are designed so that there are multiple paths between each intermediate device and the airhead, thus providing system redundancy.

In general, WMAN systems do not include security services. Therefore, DoD WMAN subscribers should assume that the WMAN system does not meet DoD security requirements and that additional security measures (e.g., VPN) are required when implementing and using these systems.

In December 2005, the IEEE 802.16 standards group approved the new IEEE 802.16e standard which will form the basis for mobile WiMAX systems. Mobile WiMAX provides the capability for users to stay connected as they move between WiMAX base stations and provides a viable wireless broadband alternative to cellular 3G systems.

2.6.4 Broadband Wireless System Compliance Requirements

Currently there are no NSA approved commercial WWAN wireless devices for storing, processing, or transmitting classified and/or SCI information.

Note: requirements in this section apply to cellular broadband systems (i.e. cellular air cards).

- *(WIR0010: CAT I) The IAO will ensure all wireless systems (including associated peripheral devices, operating system, applications, network/PC connection methods, and services) are approved by the DAA prior to installation and use for processing DoD information.*

- *(WIR0016: CAT III) The IAO will maintain a list of all DAA approved wireless devices.*

- *(WIR0040: CAT II) The IAO will ensure all wireless devices are configured according to applicable operating system STIGs.*

- *(WIR0050: CAT I) The IAO will ensure DoD licensed anti-virus software is installed on all wireless clients (e.g., laptops, PDAs, and cellular telephones) and the software is configured in accordance with the Desktop Application STIG and is kept up-to-date with the most recent virus signatures every 14 days or less. Antivirus software is NIAP Common Criteria validated as meeting U.S. Government protection profiles.*

- *(WIR0180: CAT II) The IAO will ensure wireless devices (including the SME PED) are not permitted in a permanent, temporary, or mobile SCIF unless approved in accordance with DCID 6/9 or 6/3 requirements. Local physical security operating procedures will be updated to reflect use of wireless devices in SCIFs and users will be trained on the requirements.*

- *(WIR0225: CAT II) The IAO will ensure wireless devices are not operated in areas where classified information is electronically stored, processed, or transmitted unless:*

- *Approved by the DAA in consultation with the CTTA.*

- *The wireless equipment is separated from the classified data equipment the distance determined by the CTTA and appropriate countermeasures, as determined by the CTTA, are implemented.*

- *The local physical security operating procedures will be updated to reflect use of wireless devices in SCIFs and users will be trained on the requirements.*

- *(WIR0240: CAT II) The IAO will ensure the wireless system uses two-factor authentication for identification and authentication of the user prior to connection to any DoD network. The WLAN device or keys / passwords stored on the wireless device are not used as one of the two required identification authentication factors.*

- *(WIR0373: CAT I) The IAO will ensure WWAN systems are not used to store, process, or transmit classified information.*

- *(WIR0374: CAT I) The IAO will ensure WWAN devices are not permitted in a permanent, temporary, or mobile SCIF.*

- *(WIR0378: CAT III) The IAO will ensure the requirements in the Secure Remote Computing STIG are met.*

- *(WIR0450: CAT I) The IAO will ensure password protection, which meets the following requirements, is used to protect access to device data and applications.*

- *A password meeting DoD password policies is used, if this capability is available, and the password is changed at least every 90 days.*

- *The password protection feature will not permit its bypass without zeroing all data stored on the device.*

- *The password protection feature is enabled at all times.*

- *(WIR0455: CAT II) The IAO will ensure if a WWAN PED is used to access a DoD network via the Internet through a public WWAN/Internet gateway (e.g., airport or hotel "hotspot") or cellular service provider internet gateway, the following requirements are met:*

- *The requirements in the Secure Remote Computing STIG are followed.*

- *The wireless client device has an approved personal firewall, antivirus, and VPN client installed and is operational with the latest updates installed before the wireless connection is enabled.*

- *After connecting to the hotel wireless portal or cellular Internet gateway, users are trained to immediately connect to the DoD network via the VPN client. All connections to the Internet via the hotel wireless network are through the DoD VPN connection only.*

- *Users are trained to turn-off wireless cards immediately after a VPN connection is disconnected.*

- *(WIR0460: CAT II) The IAO will ensure FIPS 140-2 certified encryption tools are used to encrypt data at rest on the wireless device.*
-
- *(WIR0490: CAT II) The IAO will ensure PDAs used for wireless Internet remote access to DoD networks meet the following standards and criteria:*

- *Data encryption meeting the FIPS 140-2 (3DES or AES) standard is used on the device.*

- *PKI certificates are used for identification and authentication of users.*

- *Only DAA approved PDAs, wireless service providers, and network access gateways are used.*

- *PDA wireless modems (e.g., IEEE 802.11, cellular, etc.) are removed or turned off when wireless data connections are not being used.*

- *DoD licensed anti-virus software is installed on the device and the software is configured in accordance with the Desktop Application STIG and is kept up-to-date with the most recent virus signatures every 14 days or less.*

- *A personal firewall is implemented on the device.*

2.7 RFID Technologies

Radio Frequency Identification (RFID) technologies are increasingly used throughout the Federal Government, primarily to facilitate inventory control of equipment, track the contents of shipping containers, or to facilitate logical access to computer systems. The DoD has been a leader in implementing RFID systems in the Federal Government.

There are two main types of RFID systems: passive and active. Passive systems store data in a small electronic device (tag) that contains electronic memory and a low power radio transmitter/receiver. The tag has no internal power. The passive tag receives radio signals received from a reader and then converts the radio signals into electrical power to transmit the data stored on the tag to the RFID reader. By contrast, active systems contain a battery and transmit stored information when queried by an RFID reader. Active systems can be designed to transmit data at distances from a few inches to a few hundred feet.

RFID transmissions can be intercepted by any receiver located within the transmit range of an RFID tag and operating on the same frequency as the tag. A RFID tag can be designed to require that the tag receive a valid passcode before stored information is transmitted. Note that reader authentication is rarely found in passive RFID systems. Since data encryption is not used with RFID systems, passcodes transmitted to RFID tags by RFID receivers are vulnerable to interception and reuse by nearby hackers.

RFID tags can contain any stored data, including user IDs and passwords. RFID tags can be designed so that the information stored on the tag cannot be modified or can be modified only by specific RFID readers, thus ensuring data integrity. Information stored on active and passive RFID tags is generally always available. Information stored on active RFID tags would not be available if the tag battery was fully discharged.

DoDD 8100.2 specifically excludes RFID devices from being covered by the wireless security requirements listed in the directive. DoD agencies should conduct a risk assessment before using RFID devices to store sensitive information.

Current DoD RFID policies do not address security and privacy of data stored on RFID tags or of data in transit while being read by an RFID scanner. (DoD RFID policies can be found at http://www.acq.osd.mil/log/rfid/rfid_policy.htm.) Industry standards have not been developed for storing encrypted data on RFID tags. Currently, there are no RFID products that provide FIPS 140-2 validated encrypted data on the tag or encrypt data in transit between the tag and reader. Several companies provide RFID systems where tag data is encrypted before it is stored on the tag.

There are three primary attack methods of RFID systems:

- A hacker may attempt to scan the tag data using a reader. Depending on the type of RFID tag used, this attack method may be relatively easy to implement. Therefore, sensitive data should not be stored on the RFID tag unless it is encrypted.

- Capture of the wireless transmission of the tag data while being read by an authorized reader. This threat is considered minimal since this attack is difficult to implement.

- Exploitation of a network via a network connected reader. This threat is considered minimal since the attack method is difficult to implement.

- *(WIR0495: CAT III) The IAO will ensure appropriate operating system and network STIGs are followed for RFID systems that connect to a DoD network.*

2.8 Free Space Optics Systems

FSO systems use light instead of radio waves to transmit broadband line of sight communications. They are usually used to provide point-to-point wireless network bridging between buildings. Data rates are typically between 100 Mbps and 1.5 Gbps with distances up to 4 kilometers. FSO communications can be adversely affected by atmospheric conditions such as fog, rain, and snow and scintillation (the "waves of heat" pattern that can occur over dark surfaces). Security requirements for FSO systems are similar to those of WLAN bridges.

- *(WIR0072: CAT II) The NSO will ensure all network devices (i.e., Intrusion Detection System (IDS), routers, Remote Access System (RAS), firewalls, etc) are located in a secure room with limited access or otherwise secured to prevent tampering or theft.*

- *(WIR0390: CAT II) The IAO will ensure FIPS 140-2 compliant encryption is used to secure the link between the two FSO terminal devices (e.g., VPN or security gateway).*

- *(WIR0391: CAT II) The IAO will ensure FSO bridges are placed in a screened subnet (DMZ or firewall separating intranet and wireless network), or VLAN and/or otherwise separated from the wired internal network. A VPN concentrator or wireless security gateway/switch is placed between the bridge and the local DoD network.*

- *(WIR0392: CAT I) The IAO will ensure management interfaces and management consoles for FSO devices are password protected and the password is compliant with DoD password policies.*

3. WIRELESS PED TECHNOLOGIES

3.1 Introduction

The use of handheld PEDs, including cell phones, 2-way pagers, PDAs, smartphones, and wireless email devices, is widespread in the DoD. Various wireless technologies are used to provide network connectivity for handheld PEDs, including cellular, broadband cellular (3G), broadband wireless, and WLAN. The convergence of mobile phone, PDA, wireless email, computer, and data storage into one handheld device has made it difficult to determine proper security requirements for these devices when used in the DoD environment.

This section will focus on cellular (including Short Messaging Service (SMS), Multimedia Messaging Service (MMS), and 2-way paging service), wireless email, and PDA operating system technologies and security features. Security requirements for handheld PEDs are consolidated at the end of the section.

3.2 Cellular Technologies, Protocols, and Security

3.2.1 Wireless Telephone Protocols

This section provides an overview of radio interface standards and protocols used by wireless carriers in the United States.

Analog wireless communications protocols, in general, provide no security services. Analog cellular calls can be easily intercepted and the Mobile Identification Number (MIN) and Electronic Serial Number (ESN) can then be extracted from the intercepted call. Analog wireless phones can be cloned using intercepted MINs and ESNs. Voice encryption services are not provided.

All digital wireless carrier systems provide device level authentication and data encryption. Some networks, such as Global System for Mobile communications (GSM), also provide user authentication.

3.2.1.1 1st Generation (1G) Technologies (Analog)

The Advanced Mobile Phone Service (AMPS) was the American analog cellular standard when deployed in the 1970s. Developed by AT&T, this standard uses Frequency Division Multiple Access (FDMA) whereby the assigned radio spectrum is divided into channels and each channel is used for either the receive or the transmit portions of the wireless phone call. See *Figure 3-1, Wireless Radio Interface Protocols*. One of the shortcomings of AMPS is the lack of inherent security features (authentication and data encryption) in the standard.

Currently, the FCC requires all U.S. cellular carriers to provide analog cellular services. In August 2002 the FCC ruled that U.S. cellular carriers could begin to phase out analog cellular services in five years.

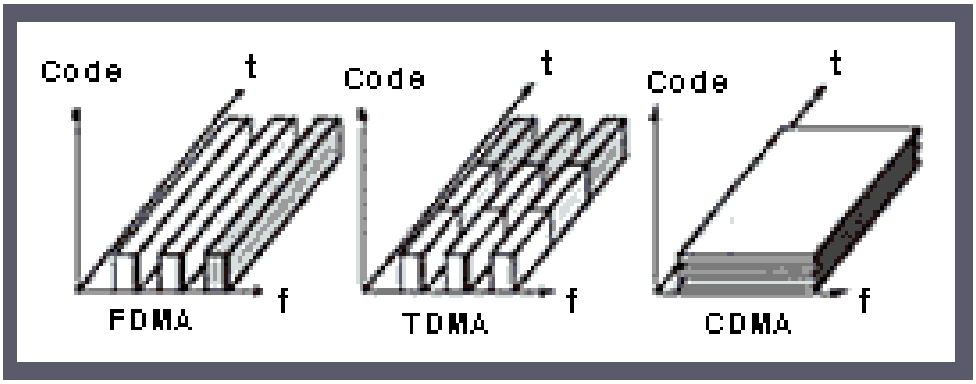

Figure 3-1. Wireless Radio Interface Protocols

- *Code division multiple access (CDMA).* TIA IS-95, published by the Telecommunications Industry Association (TIA), is the CDMA standard developed by Qualcomm. CDMA currently provides 12-16 times the channel capacity over AMPS. CDMA has been implemented by a number of national wireless carriers, including, Verizon, and Sprint Nextel PCS. CDMA provides data services with rates of about 9.6 kbps. With CDMA, the frequency spectrum is shared by all calls. Each call is assigned a pseudo random code and the receiver in both the mobile phone and base station will only accept the call with the correct code.

- *Time division multiple access (TDMA).* TDMA is the generic name for an air interface technology that is used by a number of standard digital radio systems including IS-136 and GSM. The IS-136 standard is published by the TIA and is the current United States standard for both the cellular (850 MHz) and PCS (1.9 GHz) spectrums. TDMA was implemented by a number of national wireless carriers including Cingular and AT&T Wireless. (Cingular has almost completed transitioning their TDMA customers over to their new GSM system.) Each communications channel is divided into six time slots with two being used for each wireless connection. TDMA provides a three to one gain in network capacity over an analog cellular network and data rates of about 9.6 kbps. (IS-136 is also known as D-AMPS or Digital-AMPS.)

- *Iridium.* The Iridium satellite phone system is a TDMA system but it does not operate in the cellular frequency band.

- *Global System for Mobile communications* (*GSM).* GSM is the primary digital wireless phone standard throughout the world, except for primarily North America and Japan. The 3rd Generation Partnership Project (3GPP) of the European Telecommunication Standards Institute (ETSI), a European standards group, manages the GSM standard. GSM is a form of TDMA, but it has a different timing standard than the IS-136 version of TDMA. Security features, including customer billing, authentication information, and data encryption are recorded on a Subscriber Identity Module (SIM) card, which must be inserted into the phone before a call can be sent or received. The standard GSM data rate

is 9.6 Kbps, but this capacity can be upgraded to 14.4 Kbps. T-Mobile and Cingular operate GSM networks in the U.S.

- *Integrated Dispatch Enhanced Network (iDEN).* iDEN is a TDMA based digital wireless phone technology that is used by Sprint Nextel. iDEN is a proprietary specification that was developed by Motorola and integrates four wireless services into one digital network—dispatch radio, voice, data, and short message service (SMS). Sprint/Nextel operates the only iDEN system in the U.S.

3.2.1.2 Generation (2.5G) Technologies

General Packet Radio Service (GPRS) is a packet-based digital wireless service and is considered an interim phase for GSM networks transitioning to 3G wireless systems. GPRS is deployed over GSM networks by overlaying a packet based air interface over the existing circuit-switched network. A version of GPRS has also been developed for IS-136 networks, but most U.S. based wireless carriers are using a GSM network as the foundation for their GPRS service. GPRS has maximum theoretical data rate of 171.2 Kbps with a typical user throughput of 56 – 115 Kbps. GPRS is considered an interim step from the transition of 2G wireless services to 3G. Cingular and T-Mobile have deployed GPRS service to selected markets. The European Telecommunications Standards Institute (ETSI) maintains the GPRS standard.

3.2.1.3 3rd Generation (3G) Technologies

Universal Mobile Telecommunications System (UMTS) is the International Telecommunications Union's (ITU) IMT-2000 vision for a global family of 3G wireless communications systems and consists of five 3G wireless communications standards:

- IMT-2000 CDMA Direct Spread (DS), also known as the Universal Terrestrial Radio Access (UTRA) Frequency Division Duplex (FDD) and includes WCDMA (or W-CDMA) which stands for Wideband Code Division Multiple Access. The 3rd Generation Partnership Project (3GPP) develops the Universal Mobile Telecommunications System (UMTS) and UTRA.

- IMT-2000 CDMA Multi-Carrier (MC), also known as cdma2000 (3X) was developed by 3GPP2. IMT-2000 cdma2000 includes 1X components (e.g., cdma2000 1X EV-DO).

- IMT-2000 CDMA Time Division Duplex (TDD), also known as UTRA TDD and Time Division - Synchronous Code Division Multiple Access (TD-SCDMA). TD-SCDMA was developed in China and is supported by the TD-SCDMA Forum.

- IMT-2000 TDMA Single Carrier, also known as UWC-136 Enhanced Data Rates for GSM Evolution (EDGE) which is supported by Universal Wireless Communications Consortium (UWCC).

- IMT-2000 Digital Enhanced Cordless Telecommunications (DECT) which is supported by the DECT Forum.

The IMT-2000 family of 3G systems includes three types of Core Network technologies:

- GSM based (using Mobile Application Part (MAP) protocols on top of SS7 protocols for signaling)

- ANSI-41 based (IS-634 protocols for signaling)

- Internet Protocol (IP) based

In the U.S., TDMA and GSM carriers have deployed EDGE while CDMA carriers have deployed cdma2000 1xRTT systems and started deploying cdma 1xEVDO data services in 2004. WCDMA (UMTS) and cdma2000 were developed separately and are two separate ITU approved 3G standards.

EDGE is a TDMA based 3G wireless radio interface standard that provides a migration path for GSM and IS-136 networks to 3G services. EDGE is the standard for IMT-2000 Single Carrier (also called Universal Wireless Communications-136 (UWC-136) and provides three to four times the data rates and throughput over GPRS (up to 384 Kbps theoretical with 115 Kbps considered the typical user data rate). The EDGE standard is supported by both the ITU and ETSI.

- cdma2000 is a trademark of the TIA and has been proposed as the IMT-2000 Multi Carrier standard. cdma 1xRadio Transmit Technology (1xRTT), cdma2000 1xEvolution, Data Only (1xEV-DO) and future cdma 3x were developed to be backward compatible with cdmaOne. Both 1x types have the same bandwidth and chip rate and can be used in any existing 2G cdmaOne frequency band and network. Backward compatibility was a requirement for successful deployment for the USA market. Deployment is straightforward because operators do not need new frequencies. Two versions of cdma2000 have been deployed in the United States:

    - 1xRTT CDMA will support up to 144 Kbps packet data in its first release and up to 614 Kbps in the second release. The second phase, 3x, completes the 3G evolution of the IS-95 CDMA standard. Verizon and Sprint Nextel PCS have deployed 1xRTT CDMA systems throughout the U.S.

    - 1xEV-DO Release 0 is an enhancement to cdma2000 air interface technology optimized for packet data transfer. It is one of the most promising techniques for enabling third-generation (3G) wireless communications systems to deliver IP-based services such as email, Web browsing, e-commerce and telematics. 1xEV-DO technology allows a standard 1.25 MHz cdma2000 wireless communication channel to provide a peak data rate of 2.4 Mb/sec on its forward link, effectively tripling the capacity of each cdma2000 channel. Verizon and Sprint Nextel have deployed 1xEV-DO services in numerous markets throughout the U.S. 1xEV-DO offers an "always on" user experience, so that users are free to send and receive information from the Internet and their corporate intranets, anytime, anywhere.

    - CDMA2000 1xEV-DO Revision A (Rev A) delivers peak data speeds of 3.1 Mbps on the downlink and 1.8 Mbps on the uplink and incorporates quality of service (QoS)

controls to manage latency on the network. With Rev A, operators will be able to introduce advanced multimedia services, including voice, data and broadcast over all-IP networks. Sprint Nextel and Verizon plan to 1xEV-DO Rev A, beginning in late 2006.

Wideband Code Division Multiple Access (WCDMA) is another approved 3G standard developed by DoCoMo, the dominate Japanese wireless carrier. WCDMA provides data rates up to 2 Mbps. WCDMA (UMTS) was developed mainly for countries with GSM networks, because these countries have agreed to free new frequency ranges for UMTS networks. WCDMA is a new technology and in a new frequency band, new radio access networks have to be built. The advantage is that the new frequency band gives plenty of new capacity for operators. 3GPP is overseeing the standard development and has kept the core network as close to the GSM standard as possible.

3.2.2 SMS Technology Overview

Short Messaging Service (SMS) (also called Text Messaging) is a standard protocol for GSM systems. SMS is primarily used to transmit short messages between wireless phones but also can be used to transmit a message between cell phones and computers. The SMS protocol provides no security features. Digital wireless carriers encrypt data between the phone and the carrier base station but SMS messages are not normally encrypted as they transit the wireline network.

Multimedia Messaging Service (MMS) is an advanced form of SMS that provides the capability to transmit photos, graphics, video, and other forms of multimedia. Most US wireless carriers provide MMS services.

Wireless two-way messaging services are sold by a number of wireless vendors including cellular, wireless data, and two-way paging service providers. SMS services are rarely sold as a stand-alone wireless service and are usually bundled with wireless phone, data, or email services.

3.2.3 Cell Phone Security

No cellular radio transmission is completely secure, but digital and Personal Communications Service (PCS) phones are more secure than analog phones. Conversations on analog phones can be intercepted and decoded on inexpensive and readily available radio scanners. However, conversations on digital phones are encoded, which makes them more difficult to decode when intercepted, but they are not encoded end-to-end. Digital phone conversations should always be considered unsecure since the conversation can be monitored at the cellular switch and intermediate locations in the cellular network.

- Smart card security was introduced in cellular networks by the GSM standard as Subscriber Identity Module (SIM) cards. SIM cards are designed as separate tokens located in cellular phones to hold and protect data and applications and to provide a barrier to subscription cloning. SIM card functions have been enhanced and now provide secure user authentication, data encryption, and data storage (e.g. address book) services.

Several cellular phones are now available from General Dynamics and Qualcomm to secure sensitive and classified voice and data cellular communications and meet the NSA Type-1 certification requirements:

- The Motorola Sectéra Secure GSM (SGSM) cellular phone (available from General Dynamics) provides end-to-end high assurance security over commercial GSM cellular systems. The handset is designed to support hardware clip-in modules and is compliant with the Future Narrow Band Digital Terminal (FNBDT) standard. The Sectéra Security Module utilizes the NSA Type-1 certified security core developed for Motorola's Iridium® Security Module and Sectéra Wireline Terminal. The Sectéra Wireline Terminal provides secure voice and data when connected to a standard analog handset or PC and provides a transition from STU-III to FNBDT standards. This wireline terminal produces Type-1-4 encryption with PIN access.

- The Qualcomm QSec™-800 is the first cellular phone to provide end-to-end encrypted communications using existing, commercial cellular phone networks implementing CDMA data services. This phone provides high-grade voice security and normal cell phone operation in a single handset. The QSec™-800 offers secure interoperability with STE terminals that are based on the U.S. government's FNBDT-compliant technology and equipment.

- The QSec®-2700 is a new secure cellular phone from Qualcomm. The phone provides NSA Type-1 certified secure-voice communications and secure-data connectivity and operates over 800 MHz and 1900 MHz CDMA commercial wireless networks. In addition, the QSec 2700 provides a variety of 3G CDMA2000 1X technology wireless features with data speeds up to 153 Kbps.

3.3 Wireless Two-way Paging

Wireless pagers have almost become a technology of the past, having been replaced by wireless phone messaging services. Some vendors offer paging services with two-factor authentication and FIPS 140-2 compliant 128-bit 3DES encryption. Currently, no vendors offer two-way pagers and their associated services that provide an assured channel employing NSA Type-1 certified end-to-end encryption.

3.4 Wireless Two-way Email

BlackBerry has been the most prevalent wireless email system in use in the DoD but other wireless email systems have begun to be used. Wireless email systems can expose the DoD network to significant security vulnerabilities if not configured to meet DoD security requirements. Therefore, installation and configuration of these systems must meet strict DoD security configuration guidance.[1] PED compliance requirements for wireless email systems are

[1] A consolidated list of DoD security requirements related to wireless push email systems can be found in two documents developed by DISA FSO: ***DoD Wireless Push Email System Security Requirements Matrix*** and ***DoD Bluetooth Smart Card Reader Security Requirements Matrix***. Both documents can be downloaded at http://iase.disa.mil/stigs/checklist/index.html.

found below in Paragraph 3.7.4.

The following wireless push email systems are approved for use in DoD when installed and configured in accordance with the appropriate Wireless STIG Checklist:

- Research In Motion (RIM) BlackBerry
- Apriva Sensa
- Microsoft Windows Mobile Messaging
- Motorola Good Mobile Messaging

As new wireless email systems are developed, they will be reviewed by DISA, NSA, and other appropriate DoD agencies. DISA will develop and release Wireless STIG checklists for new wireless email systems after it has been determined they meet DoD security requirements and have been approved for use in the DoD. After a wireless email system checklist has released by DISA, the system can be operated in DoD when configured according to the checklist requirements.

3.5 PDA Technologies, Protocols, and Security

PDAs can be categorized based on the OS that is used. Currently, Palm OS, developed by Palm, and Windows Mobile, developed by Microsoft, have the largest market share. Symbian, a joint venture between Ericsson, Motorola, Nokia, and Psion, developed a third operating system called Symbian OS. In addition, JAVA and Linux based PDAs are now available. Most PDA operating systems released since 2003 provide security application programming interfaces (APIs) that application developers can use to enhance the security of their applications.

PDA manufacturers include several security-related applications with their PDAs, including password protection of data on the PDA and VPN and SSL clients. In addition, add-on products with enhanced authentication capabilities, including signature, voice, and token-based authentication and data and file encryption are available from third party vendors.

3.5.1 PDA Device Security Capabilities

3.5.1.1 Palm Devices

Current versions of Palm OS (Version 5.4.9) have many enhanced security features compared to previous versions. These security features include:

- Built in Palm OS security APIs.

- Secure user authentication including support for biometrics and the Challenge Authentication Protocol (CHAP), Microsoft CHAP (MS-CHAP), and Password Authentication Protocol (PAP). Palm OS allows users to specify a set of rules (e.g., password, biometric token) that must be met in order to access the device.

- Data integrity and confidentiality encryption (128 bit). RC4 and SH-1 are included in PALM OS. Several third party vendors incorporate other cryptographic algorithms, including AES, via the Palm OS security APIs.

- Signed code support. When implemented, only applications that have a valid digital signature may access certain data and resources.

    - SSL 3.0 and VPN (IPSec and PPTP) support.

    - Device password protection. Can be set to automatically lock the device on power off, at a specific time, or after a specific period of inactivity.

    - Password protection for select records stored on the PDA.

    - Device level authentication to networks via the PDA Flash ID, Mobile Access Number (MAN), or Electronic Serial Number (ESN).

    - Certificate management APIs and support for X.509v3 certificates.

Palm OS also supports infrared, IEEE 802.11, Bluetooth, WLAN, and cellular add-on modems that are built in features of many PDA devices. Palm OS Colbalt also provides extensive Bluetooth and Smartphone support.

3.5.1.2 Windows Mobile

Windows Mobile 6.0 is the latest release of Microsoft's handheld operating system. The core operating system of Windows Mobile 6.0 is Win CE 6.0. Windows Mobile 6.0 has been released in three versions:

- Classic – For non-phone Pocket PCs.

- Standard – For non-touch screen Smartphones

- Professional – For Smartphones with touchscreens

Windows Mobile 5.0 is currently to most prevalent version of Windows Mobile and was released with the following versions;

- Pocket PC – Features include storing and retrieval of email, contacts, appointments; play multimedia files and games; exchange text messages with MSN Messenger; and browse the Web. Data can also be synchronized with a desktop computer. Pocket PC provides improved WiFi support including Zero Configuration WiFi that is similar to Wireless Zero Configuration (WZC) in Microsoft XP.

- Pocket PC Phone Edition – Combines all the standard functionality of Pocket PC with that of a feature-rich mobile phone. Provides wireless Internet access via a connection through a wireless service provider.

- Smartphone – Integrates PDA-type functionality into a voice-centric handset. Designed for one-handed handset operation with keypad access to both voice and/or data features. Optimized for voice and text communications, wireless access to Outlook information, and encrypted browsing to corporate and Internet information and services.

Windows Mobile improves security over previous versions of the WinCE platform. Microsoft has included a long alphanumeric password, but configuration settings will still permit a four-digit PIN. A user is allowed only three guesses of the password before erasing all of the data in the device's memory. Secure remote access functionality is included in Windows Mobile, including PPTP, SSL, and WTLS.

Windows Mobile includes power-on password protection and support for SSL and Private Communication Technology (PCT), the CryptoAPI 1.0 application programming interface and Windows 2000 challenge/response authentication.

Smartphone supports code signing of applications whereby any application that is downloaded is assigned to one of three trust levels:

- Privileged Trust means the application has a valid signature and a certificate that allows it access to all system resources. Very few applications should need this level of trust.

- Unprivileged Trust means the application has a valid signature, but a less trusted certificate, which means access to system resources, is restricted. Most applications will operate at this level.

- Untrusted means the application is either not signed or the certificate is not recognized. If the Smart phone enforces code signing, then such an application will not be allowed to load onto the device.

Windows Mobile 5.0 provides support for direct push wireless email service (Windows Mobile messaging) when the Messaging and Security Feature Pack (MSFP) is installed. MSFP works with Microsoft Exchange 2003 SP2. When SP2 is installed, MS Exchange can be used to push and manage security policies on wireless PDAs. New security features include remote policy enforcement, remote device wipe, password enforcement, certificate-based authentication, and S/MIME support. MSFP functions are included in Windows Mobile 6.0.

Since Windows Mobile is built on the modular WinCE operating system, each device manufacturer (HP, Dell, Casio, etc.) has the option of choosing which features to implement, therefore, not every Windows Mobile security feature may be available in a specific Windows Mobile PDA or Smartphone.

3.5.1.3 Symbian OS

Symbian OS includes a multi-tasking multithreaded core, a user interface framework, data services enablers, application engines, and integrated Personal Interface Module (PIM) functionality and wireless communications. Symbian is actively working with emerging standards, such as Java 2 Platform, Micro Edition (J2ME), Bluetooth, WAP, Multi-media Message Service (MMS), Synchronization Markup Language (SyncML), IPv6, and Wide band CDMA (WCDMA).

Symbian OS is the common core of APIs and technology that is shared by all Symbian OS phones. Symbian OS includes a multi-tasking kernel, middleware for communications, data management and graphics, the lower levels of the GUI framework, and application engines. Symbian OS security includes full-strength encryption and certificate management; secure communications protocols (including HTTPS, WTLS, and SSL); and certificate-based application installation.

Substantial security features were added in Symbian OS Version 6.0 (and included in subsequent versions. Version 9.3 is the latest release), primarily in two modules—the cryptography module and the certificate management module. Security features include standard cryptography algorithms, hash key generation, random number generation, and certificate management. The certificate management module certificate lifecycle services include storage and retrieval of certificates, assignment of trust status to a certificate on an application-by-application basis, certificate chain construction and validation, and verification of trust of a certificate.

3.5.1.4 Wireless Java

The Java Technology for the Wireless Industry (JTWI) specification defines the version of the Java operating system for mobile devices. The latest edition of the Java toolkit (Sun Java Wireless Toolkit 2.5), used by developers to build wireless Java applications and Java operating system packages for PDAs, contains a set of security APIs that provide the following features:

- Permissions and Code Signing – These APIs verify that an application is signed with a trusted digital signature. Access to resources and network connections are granted based on the digital signature verification.

- Server Authentication.

- SSL and TLS data encryption services.

NOTE: Security features available in a specific wireless Java PDA will depend on what security features the PDA vendor has implemented.

3.5.1.5 Linux

Many PDA developers believe that Linux is a better choice for mobile devices than other mobile/wireless operating systems because the operating system supports numerous installation methods that work in many heterogeneous environments and needs smaller resources.

A wide range of security features are available in Linux PDAs because vendors can include any available Linux operating system authentication, access control, and encryption security component or include various Linux security applications in their product.

3.5.2 On-Device File Encryption

The first line of defense for protecting data stored in mobile devices is the power-on password that comes built into the device. The second line of defense is to encrypt the data on the device (data-at-rest encryption). These actions mitigate the risk of data compromise attacks where an attacker has physical access to a lost or stolen PDA. Several vendors offer products that encrypt selected applications, content, and passwords on the device and support AES 128-bit encryption. FIPS 140-2 certified PDA file/data encryption products are available from several vendors.

3.5.3 Tethered Modem

Many PDAs and Smartphones can function as a "tethered modem". In this configuration, a laptop computer is connected to the PDA/Smartphone and the radio of the PDA/Smartphone is used as a wireless modem connecting the laptop to the Internet. Prior to using a PDA or Smartphone as a tethered modem, review the manufacturer specifications to verify that data transmitted over the modem is not written to the PDA/Smartphone while operating in the tethered modem mode.

3.6 SME PED

The Secure Mobile Environment Portable Electronic Device (SME PED) is currently under development by the NSA and will be a converged voice and data, unclassified and classified cell phone, wireless email, and computing device. This device will similar in form factor to a PDA and Smartphone. The SME PED is targeted towards two types of Government users: a user that processes sensitive (e.g., FOUO, Privacy Act) voice and data communications and a user that processes both classified and unclassified voice and data communications. The SME PED includes the following features.

Unclassified, Non Type 1 User:

- Appointments, address book, office applications and other personal data
- Access web, email and voice anywhere in the world
- Protected voice and data

Classified Type 1 Plus Unclassified Non Type-1 User:

- Unclassified appointments, address book, office applications and other personal data current and continuous
- Unclassified access web, email and voice anywhere in the world
- Unclassified protected voice and data

- Secure (TS) voice
- Secure (SECRET) email/web browsing
- Classified documents, addresses and calendars (even at rest)
- Multiple independent levels of security
- Interoperability with DHS/unclassified networks and users

Both General Dynamics C4S and L-3 Communications were selected by NSA to develop the SME PED. The first prototype devices are expected to be available for performance and interoperability testing in November 2006 and initial product availability is expected in June/July 2007.

3.7 PED Compliance Requirements

3.7.1 Requirements for All PEDs (Classified and Unclassified Systems)

- *(WIR0010: CAT I) The IAO will ensure all wireless systems (including associated peripheral devices, operating system, applications, network/PC connection methods, and services) are approved by the DAA prior to installation and use for processing DoD information.*
- *(WIR0011: CAT III) The IAO will ensure personally owned PEDs are not used to transmit, receive, store, or process DoD information unless approved by the DAA and the owner signs forfeiture agreement in case of a security incident.*
- *(WIR0012: CAT III) The IAO will ensure all PDAs display the following banner during device unlock/ logon: "I've read & consent to terms in IS user agreement."*
- *(WIR0016: CAT III) The IAO will maintain a list of all DAA approved wireless devices.*
- *(WIR0030: CAT III) The IAO will ensure wireless devices connecting directly or indirectly (e.g., hotsync, wireless) to the network are added to site SSP.*
- *(WIR0076: CAT III) For mobile and remote users of the DoD enclave and resources, the IAM will develop a written security policy or checklist for secure wireless remote access to the site and an agreement between the site and remote user. These documents will include relevant security requirements, including (but not limited to) the following.*

- *The agreement will contain the type of access required by the user (privileged, end-user, etc.).*
- *The agreement will contain the responsibilities, liabilities, and security measures (e.g., malicious code detection training) involved in the use of the wireless remote access device.*

- *Incident handling and reporting procedures will be identified along with a designated point of contact.*

- *The remote user can be held responsible for damage caused to a Government system or data through negligence or a willful act.*

- *The policy will contain general security requirements and practices and are acknowledged and signed by the remote user.*

- *If classified devices are used for remote access from an alternative work site, the remote user will adhere to DoD policy in regard to facility clearances, protection, storage, distributing, etc.*

- *Government owned hardware and software is used for official duties only. The employee is the only individual authorized to use this equipment.*

DoD CIO Memorandum "Policy on Use of Department of Defense (DoD) Information Systems Standard Consent Banner and User Agreement," dated 2 Nov 2007 requires the following additional information in all User Agreements:

STANDARD MANDATORY NOTICE AND CONSENT PROVISION FOR ALL DOD INFORMATION SYSTEM USER AGREEMENTS
By signing this document, you acknowledge and consent that when you access Department of Defense (DoD) information systems:

- *You are accessing a U.S. Government information system (as defined in CNSSI 4009) that is provided for U.S. Government-authorized use only.*

- *You consent to the following conditions:*
  - *The government routinely monitors communications occurring on this information system, and any device attached to this information system, for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network defense, quality control, employee misconduct investigations, law enforcement investigations, and counterintelligence investigations.*
  - *At any time, the government may inspect and/or seize data stored on this information system and any device attached to this information system.*
  - *Communications occurring on or data stored on this information system, or any device attached to this information system, are not private. They are subject to routine monitoring and search.*
  - *Any communications occurring on or data stored on this information system, or any device attached to this information system, may be disclosed or used for any U.S. Government-authorized purpose.*
  - *Security protections may be utilized on this information system to protect certain interests that are important to the government. For example, passwords, access cards, encryption or biometric access controls provide security for the benefit of the government. These protections are not provided for your benefit or privacy and may be modified or eliminated at the government's discretion.*

- *(WIR0180: CAT II) The IAO will ensure wireless devices are not permitted in a permanent, temporary, or mobile SCIF unless approved in accordance with DCID 6/9 or 6/3 requirements.*

- *(WIR0370: CAT II) The IAO will ensure PEDs are allowed or operated in areas where classified discussions or data processing takes place only when:*

- *The DAA, in consultation with the CTTA, has approved cellular devices can be brought into the facility and/or used in the facility.*

- *The device's voice recording capability is rendered inoperable.*

- *The cellular devices are separated from the classified data equipment at a distance determined by the CTTA and appropriate countermeasures, as determined by the CTTA, are implemented.*

- *Wireless devices are not connected via hot-sync to a workstation in a SCIF.*

- *(WIR0372: CAT I) The IAO will ensure PEDs with digital cameras (still and video) are not allowed in any SCIF or other area where classified documents or information is stored, transmitted, or processed.*

- *(WIR0371: CAT III) The IAO will ensure PEDs with digital cameras (still and video) are allowed in a DoD facility only if specifically approved by site physical security policies.*

- *(WIR0410: CAT II) The IAO will ensure PEDs are not connected to any workstation that stores, processes, or transmits classified data unless the PED uses NSA Type-1 data-at-rest encryption and is approved by NSA for the storage of classified information.*

NOTE: Currently (August 2007), there are no PEDs that are NSA-certified for processing classified information.

- *(WIR0450: CAT I) The IAO will ensure password protection, which meets the following requirements, is used to unlock the device and access device data and applications.*

- *A password meeting DoD password policies is used, if this capability is available, and the password is changed at least every 90 days.*

- *The password protection feature will not permit its bypass without zeroing all data stored on the device.*

- *The password protection feature is enabled at all times.*

NOTE: Smart Card Login (SCL) using a DoD CAC is the preferred method for user authentication to unlock a handheld PED that sends, receives, or stores DoD information or is used to remotely access DoD networks (via a VPN, thin client (e.g.

Citrix), Outlook Web Access, wireless push email, etc.). It is strongly recommended that organizations first pilot this capability, to ensure that the second and third order effects are known and any operational impacts are mitigated (i.e. forgotten CACs, battery drained or broken readers, etc.).

- *(WIR0465: CAT II) The IAO will ensure mobile code is not downloaded from non-DoD sources and is downloaded from only trusted DoD sources over assured channels.*

- *(WIR0470: CAT II) The IAO will ensure that PEDs that are used in areas where DoD information is processed:*

- *Have IR ports disabled when IR transmissions are not being used.*

- *Data exchange via the IR port should be limited to trusted DoD devices.*

- *The local CSA CTTA should be consulted to determine appropriate method for disabling the IR port on the PDA.*

3.7.2 Additional Requirements for PEDs Processing Classified Information

Currently, the only handheld PEDs authorized to process classified information are the cellular phones listed in Section 3.2.3.

- *(WIR0394: CAT I) The IAO will ensure PEDs are not used to access secure (classified) WLANs.*

- *(WIR0350: CAT I) The IAO will ensure only NSA Type-1 certified cellular or satellite phones are used for classified voice or classified data wireless telephone transmissions. The classification level of information transmitted over the phone will not exceed the classification level approved for the phone.*

- *(WIR0380: CAT I) The IAO will ensure PDAs used to transmit, receive, store, or process Classified data use NSA, Type1 certified end-to-end encryption for data being transmitted, received, stored, or processed.*

- *(WIR0420: CAT II) The IAO will ensure synchronization software is not loaded on systems processing classified information. (Classified information will not be synched. PDAs will not be connected via hot-sync to a classified workstation.)*

- *(WIR0425: CAT II) The IAO will ensure classified data stored on PEDs is encrypted using NSA Type 1 certified encryption consistent with the classification level of the data stored on the device.*

3.7.3 Additional Requirements for PEDs Processing Unclassified Information

- *(WIR0050: CAT I) The IAO will ensure DoD licensed anti-virus software is installed on all wireless clients (e.g., laptops, PDAs, and cellular telephones) and the software is configured in accordance with the Desktop Application STIG and is kept up-to-date with the most recent virus signatures every 14 days or less. Antivirus software is NIAP Common Criteria validated as meeting U.S. Government protection profiles.*

- *(WIR0100: CAT III) The IAO will ensure a personal firewall is implemented on each 802.11-enabled wireless device to block unauthorized access to the device and the software is configured in accordance with the Desktop Application STIG. Personal firewall software is NIAP Common Criteria validated as meeting U.S. Government protection profiles.*

- *(WIR0240: CAT II) The IAO will ensure the wireless system uses two-factor authentication for identification and authentication of the user prior to connection to any DoD network. The WLAN device or keys / passwords stored on the wireless device may not be used as one of the two required identification and authentication factors.*

- *(WIR0365: CAT II) The IAO will ensure that if a PED is used to access an unclassified WLAN, the following requirements are implemented: WIR0100, WIR0130, WIR0161, WIR0167, WIR0240, WIR0260, and WIR0270.*

- *(WIR0455: CAT II) The IAO will ensure if a PED is to be used to access a DoD network via the Internet through a public WLAN/Internet gateway (e.g., airport or hotel "hotspot") or cellular service provider internet gateway, the following requirements are met:*

  - *The requirements in the Secure Remote Computing STIG are followed.*

  - *The wireless client device has an approved personal firewall, antivirus, and VPN client installed and is operational with the latest updates installed before the wireless connection is enabled.*

  - *After connecting to the hotel wireless portal or cellular Internet gateway, users will be trained to immediately connect to the DoD network via the VPN client. All connections to the Internet via the hotel wireless network will be through the DoD VPN connection only.*

  - *Users will be trained to turn-off wireless cards immediately after a VPN connection is disconnected.*

- *(WIR0340: CAT III) The IAO will ensure if non-secure (devices are not FIPS 140-2 certified or NSA Type-1 certified) cellular phones, cordless phones, and two-way radios are used for voice communications, users are trained not to discuss sensitive information over these devices.*

- *(WIR0460: CAT II) The IAO will ensure FIPS 140-2 certified encryption tools are used to encrypt data at rest on the wireless device.*

- *(WIR0480: CAT II) The IAO will ensure all PDA hotsync operations meet the following conditions:*

- *Hot-sync management software uses some form of access control (e.g., user password is entered before a hotsync operation can be executed).*

- *The user disables wireless operations when a PDA is connected to the DoD wired network via a hotsync or other interface cable.*

- *PDAs that transmit, receive, store, or process DoD information are not synced to home or personally owned PCs.*

- *(WIR0490: CAT II) The IAO will ensure PDAs used for wireless Internet remote access to DoD networks meet the following standards and criteria:*

- *Data encryption meeting the FIPS 140-2 (3DES or AES) standard is used on the device.*

- *Only DAA approved PDAs, wireless service providers, and network access gateways are used.*

- *PDA wireless modems (e.g., IEEE 802.11, cellular, etc.) are removed or turned off when wireless data connections are not being used.*

- *(WIR0540: CAT III) The IAO will ensure that if PEDs are used to send or receive cellular Short Messaging Service (SMS) and Multimedia Messaging Service (MMS) messages, only unclassified, public releasable (i.e., not FOUO, sensitive information, or Classified) information will be sent or received.*

- *(WIR0545: CAT II) The IAO will ensure an IT policy manager is used to centrally manage the security policy on handheld PEDs used for wireless remote connections (e.g. VPN, thin client (e.g. Citrix), Outlook Web Access via WLAN, cellular, etc.) to DoD networks or to send, receive, or save in memory DoD information, including email. The IT policy manager will be configured to control the following functions on the PED:*

- *Enable/disable wireless services (IR, Bluetooth, WLAN, cellular, etc.).*

- *Enable/disable camera and voice recording.*

- *Select user authenticated logon to the device via password/PIN or Smart Card Login (SCL) (user cannot bypass device authentication).*

- *When password authentication is enabled, the handheld device will automatically perform a "Data Wipe" command after X number of unsuccessful password*

authentication attempts. The value of X is set by IT policy management control. Data Wipe will delete all data/information in addressable memory on the device.

- *Password authentication setting of the IT policy manager is configurable as needed to meet both DoD and local mission requirements. Thus, the following features are required:*
    - *Ability to set maximum password age (e.g. 30 days, 90 days, 180 days)*
    - *Ability to set minimum password length. A range of 5 to 12 characters is the minimum requirement.*
    - *Ability to set maximum password attempts. Device will perform a Data Wipe after a set number of incorrect passwords are entered. A range of 3-10 incorrect passwords before a Data Wipe is performed is the minimum requirement.*
    - *Ability to set minimum password history (0-5 is the minimum requirement)*
- *The handheld device inactivity timeout setting will be configurable to between 3 to 60 minutes range). This setting requires the user to unlock the device by reentering their password or Smart Card PIN after the configured period of inactivity. The administrator will choose a specific setting based on mission/user requirements, however, a setting of 15 minutes is recommended based on current NSA operating system inactivity requirements.*
- *The system shall control the capability of the user to install or de-install third party applications on the handheld device.*
- *If SCL is supported, the Smart Card Reader (SCR) is fully interoperable with DoD PKI and CAC.*

NOTE: The following features are required by DoD policy but can be implemented using other techniques other than the IT Policy Manager. Therefore, these features are desirable but not required features of the IT Policy Manager:

- Verify data-at-rest encryption on device.
- Verify anti-virus/personal firewall software is installed on handheld PED and kept up-to-date.
- Notify user when operating system software and critical application software updates are available.

PEDs should only be purchased after verifying that file encryption software is available for that equipment. PEDs that are used for wireless Internet remote access to DoD networks should only be purchased after it has been verified that FIPS 140-2 certified data encryption software, anti-virus software, and personal firewall software is available for that equipment. PEDs with

Bluetooth radios should not be purchased unless the Bluetooth radio transmission can be secured with FIPS 140-2 certified data encryption software or the Bluetooth radio can be removed or disabled.

3.7.4 Requirements for Wireless Push Email PEDs

The following general wireless system requirements apply to all wireless push email systems: WIR0010, WIR0011, WIR0016, WIR0030, WIR0076, WIR0180, WIR0225, WIR0371, and WIR0372.

The following requirements apply to all DoD wireless push email systems and are described in detail in the appropriate wireless push email system checklist (e.g. Blackberry, etc.) and not in the Wireless Checklist.

- *(WIR1010: CAT II) The IAO will ensure if a CMI occurs on a wireless push email PED, the procedures found in the appropriate system checklist are followed.*

- *(WIR1015: CAT II) The IAO will ensure, prior to disposing of a wireless email handheld PED (e.g. sold, transferred to another DoD or other government agency, etc.), the procedures found in the appropriate wireless push email system checklist are followed.*

- *(WIR1020 CAT I) The IAO will ensure wireless email devices and systems are not used to send, receive, store, or process classified messages unless the PED uses NSA Type-1 data-at-rest and data-in-transit encryption and is approved by NSA for the storage and transmission of classified information.*

- *(WIR1040 CAT I) The IAO will ensure that wireless email devices and systems are not connected to classified DoD networks or information systems.*

- *(WIR1070: CAT I) The IAO will ensure only the wireless push email system uses only approved hardware and software versions and approved email redirection methods, as described in the appropriate system checklist.*

- *(WIR1080: CAT I) The IAO will ensure that the wireless push email system network architecture will comply with the approved architecture described in the appropriate system checklist.*

- *(WIR1090: CAT II) The IAO will ensure the system administrator sends a Data Protection Command (e.g. "Data WIPE") to the device and removes the device from the email management server when a wireless push email device is reported lost or stolen.*

- *(WIR1100: CAT I) The IAO will ensure the wireless push email device is protected by authenticated login procedures to unlock the device. This can be accomplished by using password (PIN) protection or by using Common Access Card (CAC)/PKI authentication.*
- *When password protection only is implemented, the following procedures are enforced.*

- *The device password (PIN) is set to five or more characters. The wireless email management server is configured to enforce this policy. If five characters are used, both a letter (lower case or upper case) and a number are used in all device passwords (the BES is configured to enforce this policy). If six or more characters are used, numbers only may be used for the password. It is recommended that eight or more characters be used.*

- *The number of incorrect passwords entered before a device wipe occurs is set to 10 or less. The wireless email management server is configured to enforce this policy.*

- *The password is changed at least every 90 days. The wireless email management server is configured to enforce this policy.*

When CAC/PKI authentication is implemented, the procedures found in the appropriate system checklist are followed.

- *(WIR1110: CAT I) The IAO will ensure when an application is used on a wireless email device to store passwords, the DAA has reviewed and approved its use, and the application is configured as described in the appropriate system checklist.*

- *(WIR1120: CAT II) The IAO will ensure all wireless push email devices are set to lock (timeout) after 15 minutes or less of inactivity.*

- *(WIR1130: CAT I) The IAO will ensure when a wireless email management server (e.g. BES MDS, Windows Mobile Messaging with Exchange) is used to provide user access to internal DoD network web servers, CAC user authentication is enabled on the web server and user access is restricted to authorized servers only.*

- *(WIR1140: CAT II) The IAO will ensure a wireless push email device, which has a Bluetooth radio, applies the following Bluetooth controls.*

- *Bluetooth data transmissions (e.g. syncing to the desktop or transfer of data files) on BlackBerry devices are disabled except for the authorized Bluetooth CAC reader (i.e. Bluetooth Smart Card reader (SCR)). Only NSA or DISA tested and approved SCRs may be used.*

- *Bluetooth for voice transmissions (e.g. Bluetooth ear bud) is not authorized. Both the Bluetooth Handsfree and Headset profiles are disabled by the wireless push email server security policy configuration. Users should use wired handsfree devices.*

- *(WIR1150: CAT III) The IAO will ensure when a Bluetooth smart card reader (SCR) is used with a wireless email device, the procedures found in the appropriate system checklist are followed. Only DISA approved Bluetooth SCRs can be used.*

- *(WIR1160: CAT II) The IAO will ensure all host servers and computers where wireless push email management software is installed (e.g., BES, email server, and LDAP server) are hardened in accordance with the appropriate operating system STIG.*

- *(WIR1170: CAT II) The IAO will ensure the system administrator performs a hard reset command (e.g. "Wipe") on all new or reissued wireless push email handheld devices and that an IT policy is pushed to the device before issuing it to DoD personnel and placing the device on a DoD BlackBerry network. Procedures listed in the appropriate checklist must be followed.*

- *(WIR1180: CAT I) The IAO will ensure wireless push email device users can not install or remove applications and/or software on their handheld device, unless the process is directed by the IAO and under the supervision of an authorized system administrator. Enforcement must be via system security policy. Procedures listed in the appropriate checklist must be followed.*

- *(WIR1190: CAT I) The IAO will ensure JTF-GNO prohibited applications are not installed on wireless email servers or handheld devices.*

- *(WIR1200: CAT II) The IAO will ensure that all wireless push email emergency and/or critical email notifications are digitally signed and verified to ensure the authenticity of the sender.*

- *(WIR1210: CAT III) The IAO will ensure that if wireless push email auto signatures are used, the signature message does not disclose that the email originated from a mobile device (e.g., "Sent From My BlackBerry Wireless Handheld").*

- *(WIR1220: CAT II) The IAO will ensure security requirements for Short Message Service (SMS), Multi-media Messaging Service (MMS), Pin-To-Pin messaging, and other text messaging services are followed as described in the appropriate wireless email system checklist.*
-
- *(WIR1230: CAT II) The IAO will ensure that the following procedures are implemented for wireless email device Over-the-Air (OTA) activation:*

- *Wireless email device users are not allowed to OTA activate their handheld device unless under the direction of the system administrator.*

- *OTA activation is implemented as directed in the appropriate wireless push email system checklist.*

- *(WIR1240: CAT II) The IAO will ensure that the wireless email device is configured to require all Internet browsing to occur via a DoD controlled web server/proxy. Procedures listed in the appropriate checklist must be followed.*

- *(WIR1250: CAT II) The IAO will ensure all required wireless push email management server and handheld device settings listed in the appropriate system checklist are implemented.*

- *(WIR1260: CAT I) The IAO will ensure that the wireless link encryption key be automatically changed at least every 30 days or less by the wireless email management server.*

- *(WIR1270: CAT II) The IAO will ensure that local security policies include requiring the wireless email handheld device be cradled or synced at least once every 30 days to the wireless email server to receive updated keys and/or software updates on a frequent basis.*

- *(WIR1280: CAT III) The IAO will ensure that Data-at-Rest encryption is enabled on all wireless push email handheld devices using FIPS 140-2 certified encryption.*

APPENDIX A. RELATED PUBLICATIONS

Applicable Federal Policies and Guidelines

NIST Special Publication 800-46 "Security For Telecommuting and Broadband Communications," August 2002, (http://csrc.nist.gov/publications/nistpubs/index.html)

NIST Special Publication 800-48, Wireless Network Security: 802.11, Bluetooth, and Handheld Device, November 2002, (http://csrc.nist.gov/publications/nistpubs/index.html)

OMB Circular A-130, Management of Federal Information Resources (http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html)

Applicable DoD Policies and Guidelines

Enclave Security STIG

Network Infrastructure STIG

Secure Remote Computing STIG

Desktop STIG

Internet Protocol Telephony and Voice Over Internet Protocol STIG

DoD Directive 8100.2, Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG), 14 April 2004.

ASD-NII Memorandum, Subject: Use of Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies in the Department Defense (DoD) Global Information Grid (GIG), 2 June 2006.

DoD Directive 8500.1, Information Assurance, 24 October 2002.

DISA Director's Policy Letter 2003-7, Portable Electronic Devices, 1 July 2003.

DoD Instruction 8500.2, Information Assurance (IA) Implementation, 6 February 2003.

Office of the Secretary of Defense Memorandum, Department of Defense (DoD) Information Assurance Vulnerability Alert (IAVA).

NSA Secure Wireless LAN CONOPS, Version 1.0, March 2004 (FOUO).

Committee on National Security Systems Instruction 3034, Operational Security Doctrine for SECNET 11 Wireless Area Network Interface Card, April 2004 (FOUO).

NSA/CSS Policy Manual 9-12, NSA/CSS Storage Device Declassification Manual, 13 March 2006. (U/FOUO).

Preliminary Security Evaluation of RIM's BlackBerry-to-Smart Card Reader Bluetooth Interface, Headquarters Army Materiel Command (AMC) Report, 7 April 2006 (U/FOUO).

Technical Evaluation of RIM's Smart Card Reader, BlackBerry Bluetooth Support, and Bluetooth Headsets; NSA; I332-013R-2006; 12 May 2006 (SECRET).

Technical Evaluation of Apriva's BT100-C Bluetooth Universal Smart Card Reader with Supported Handheld Devices, NSA, I732-023R-2006, 13 December 2006 (U/FOUO).

APPENDIX B. IAVM COMPLIANCE

IAVM Wireless Related Notices

JTF-GNO Cyber Alert 074-06, BlackBerry and PDA Configuration Requirements, 7 Nov 2006 (Unclass/FOUO).

This page intentionally blank

APPENDIX C. LIST OF ACRONYMS

AAA	Authentication, Authorization, and Accounting
ACL	Access Control List
AES	Advanced Encryption Standard
AIS	Automated Information Systems
AMPS	Advanced Mobile Phone Service
ANSI	American National Standards Institute
API	Application Program Interface
ARP	Address Resolution Protocol
ASDC3I	Assistant Secretary of Defense for Command, Control, Communications, and Intelligence
BES	BlackBerry Enterprise Sever
BRAN	Broadband Radio Access Network
C2	Level C Security for Computer Products (provides Discretionary Access Control [DAC])
C&A	Certification and Accreditation
CA	Certificate Authority
CAC	Common Access Card
CCI	Co-channel Interference
CCMP	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
CDG	CDMA Development Group
CDMA	Code Division Multiple Access
CDPD	Cellular Digital Packet Data
CF	Compact Flash
CGI	Common Gateway Interface
CHAP	Challenge Authentication Protocol
CICS	Customer Information Control System
CJCS	Chairman, Joint Chiefs of Staff
CMI	Classified Message Incident
CMOD	Cryptographic Modules
CC/S/A	Combatant Commanders/Services/Agencies
COMSEC	Communications Security
COTS	Commercial-Off-The-Shelf
CRT	Display Monitor (Cathode Ray Tube)
CSA	Command, Service, and Agency
CSA	Cognizant Security Authority
CTIA	Cellular Telecommunications & Internet Association
CTTA	Certified TEMPEST Technical Authority
DAA	Designated Approving Authority
DAC	Discretionary Access Control
dBi	Decibel (measure of antenna gain in decibels)

DCID	Director of Central Intelligence Directive
DECC	Defense Enterprise Computing Center
DECC-D	Defense Enterprise Computing Center-Detachment
DES	Data Encryption Standard
DH	Diffie Hellman
DISA	Defense Information Systems Agency
DISAI	DISA Instruction
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
DoD	Department of Defense
DOS	Denial of Service
DSAWG	Defense Security Accreditation Working Group
DSL	Digital Subscriber Line
DSSS	Direct Sequence Spread Spectrum
EAL	Evaluation Assurance Level
EAP	Extensible Authentication Protocol
EAS	Extended Assistance Support
ECC	Eliptic Curve Cryptography
EDGE	Enhanced Data Rate for Global Evolution
EESS	Earth Exploration Satellite Service
EIA	Electronic Industry Association
EIR	Equipment Identity Register
Email	Electronic Mail
EMS	Extended Maintenance Support
ESAF	External Subsystem Attachment Facility
ESN	Electronic Serial Number
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
FHSS	Frequency Hopping Spread Spectrum
FIPS	Federal Information Processing Standard
FNBDT	Future Narrow Band Digital Terminal
FSO	Field Security Operations
FSO	Free Space Optics
FWPC	Federal Wireless Policy Committee
FWUF	Federal Wireless Users Forum
GHz	Gigahertz
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
HSCSD	High-Speed Circuit-Switched Data
HTML	Hyper Text Markup Language
HTTP	Hyper Text Transport Protocol
HTTPS	Hyper Text Transport Protocol - Secure

I&A	Identification and Authentication
IAM	Information Assurance Manager
IAO	Information Assurance Officer
IAPP	Inter-Access Point Protocol
IASE	Information Assurance Support Environment
IAVA	Information Assurance Vulnerability Alert
iDEN	Integrated Dispatch Enhanced Network
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IMEI	International Mobile Equipment Identity
INFOCON	Information Operations Condition
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSec	IP Security
IR	Infrared
IrDA	Infrared Data Association
ISA	Industry Standard Architecture
ISM	Industrial, Scientific, and Medical
ISO	International Standards Organization
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
IT	Iinformation Technology
ITU	International Telecommunications Union
IV	Initialization Vector
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LEAP	Lightweight EAP
MAC	Media Access Control
MBPS	Megabits Per Second
MD5	Message Digest 5
MDS	Mobile Data Service
MIC	Message Integrity Check
MIMO	Multiple-Input Multiple-Output
MIN	Mobile Identification Number
MS-CHAP	Microsoft CHAP
MMS	Multi-Media Message Service
NETSEC	Network Security
NIC	Network Interface Card
NIPRCAP	NIPRNet Connection Approval Process
NIPRNet	Non-classified (but Sensitive) Internet Protocol Routing Network
NIAP	National Information Assurance Partnership

NIST	National Institute of Standards and Technology
NSO	Network Security Officer
NSA	National Security Agency
NTLM	Windows NT LAN Manager
OCB	Offset Codebook
OCSP	Online Certificate Status Protocol
OFDM	Orthogonal Frequency Division Multiplexing
OS	Operating System
OSI	Open Systems Interface
OUS&P	Outside United States and Possessions
PAN	Personal Area Network
PAP	Password Authentication Protocol
PCI	Peripheral Component Interconnect
PCIA	Personal Communications Industry Association
PCMCIA	Personal Computer Memory Card International Association
PCS	Personal Communications Service
PCT	Private Communication Technology
PDA	Personal Digital Assistant
PEAP	Protected Extensible Authentication Protocol
PED	Personal Electronic Device
PIM	Personal Interface Module
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PKIX	Public-Key Infrastructure X.509
POS	Personal Operating Space
PPP	Point-to-Point-Protocol
PPTP	Point-to-Point Tunnel Protocol
QoS	Quality of Service
RADIUS	Remote Access Dial-in User Service
R & D	Research and Development
RF	Radio Frequency
RFID	Radio Frequency Identification
RIM	Research in Motion
RMOD	Radio Module
RSN	Robust Security Network
SA	System Administrator
SCAO	SIPRNet Connection Approval Office
SCI	Sensitive Compartmented Information
SCL	Smart Card Login (SCL)
SCIF	Sensitive Compartmented Information Facility

SCR	Smart Card Reader
SGSM	Secure GSM
SHA	Secure Hash Algorithm
SID	System Identifier
SIG	Special Interest Group
SIM	Subscriber Identity Module
SIPRNet	Secret Internet Protocol Router Network
SM	Security Manager
SME PED	Secure Mobile Environment Portable Electronic Device
S/MIME	Secure Multipurpose Internet Mail Extensions
SMS	Short Message Service
SNMP	Simple Network Management Protocol
SRR	Security Readiness Review
SRRDB	SRR Database
SRS	Space Research Service
SRP	Server Router Protocol
SSAA	System Security Authorization Agreement
SSID	Service Set Identifier
SSL	Secure Sockets Layer
SSN	Subsystem Name
SSP	Site Security Plan
STE	Secure Terminal Equipment
STIG	Security Technical Implementation Guide
TCP	Transmission Control Protocol
TDMA	Time Division Multiple Access
TIA	Telecommunications Industry Association
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TTLS	Tunneling TLS
UMTS	Universal Mobile Telecommunications System
UNII	Unlicensed National Information Infrastructure
US&P	United States & Possessions
USB	Universal Serial Bus
VCTS	Vulnerability Compliance Tracking System
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAP	Wireless Application Protocol
WCDMA	Wide band CDMA
WECA	Wireless Ethernet Compatibility Alliance
WEP	Wired Equivalent Privacy
WID	Wireless Information Device
Wi-Fi	Wireless Fidelity

WIM	WAP Identity Module
WISP	Wireless Internet Service Provider
WLAN	Wireless LAN
WLANA	Wireless LAN Association
WMAN	Wireless Metropolitan Area network
WPA	Wireless Protected Access
WPA2	Wireless Protected Access 2
WPAN	Wireless Personal Area Network
WPKI	WAP or Wireless Public Key Infrastructure
WRAP	Wireless Robust Authentication Protocol
WTLS	Wireless Transport Layer Protocol
WWAN	Wireless Wide Area Network
WWW	World Wide Web
WZC	Wireless Zero Configuration
XMOD	External Modules